ZyXEL

Firmware Release Note

ZyWALL USG 50

Release 3.00(BDS.4)C0

Date: Jan. 18, 2013

Author: Jacko Cheng

Project Leader: Jacko Cheng

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

ZyXEL ZyWALL USG 50

Release 3.00(BDS.4)C0

Release Note

Date: Jan. 18, 2013

Supported Platforms:

ZyXEL ZyWALL USG 50

Versions:

ZLD Version: V3.00(BDS.4) | 2013-01-18 16:59:36
BootModule Version: V1.17 | 12/01/2011 05:20:17

Files lists contains in the Release ZIP file

File name: 300BDS4C0.bin

Purpose: This binary firmware image file is for normal system update.

Note: The firmware update may take five or more minutes depending on the scale of device configuration. The more complex configuration will take more update time. Do not turn off or reset the ZyWALL while the firmware update is in progress. The firmware might get damaged, if device loss power or you reset the device during the firmware upload. You might need to refer to Appendix 3 of this document to recover the firmware.

File name: 300BDS4C0.conf

Purpose: This ASCII file contains default system configuration commands.

File name: 300BDS4C0.pdf

Purpose: This release file.

File name: 300BDS4C0.ri

Purpose: This binary firmware recovery image file is for emergent system firmware damage recovery only.

Note: The ZyWALL firmware could be damaged, for example by the power going off or pressing Reset button during a firmware update.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

File name: 300BDS4C0-enterprise.mib, 300BDS4C0-private.mib

Purpose: The Enterprise and Private MIBs are to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

File name: firmware.xml

Purpose: This file is needed by ZyXEL Centralized Network Management (CNM) 3.0 or after.

File name: 300BDS4C0-opensource-list.xls

Purpose: This file lists the open source packages.

Read Me First

1. The system default configuration is summarized as below:
   - The default device administration username is “admin”, password is “1234”.
   - The default LAN interface is lan1, which are P3 and P4 ports on the front panel. The default IP address of lan1 is 192.168.1.1/24.
   - By default, WWW/SSH/SNMP service can only be accessed from LAN subnet.
   - The default WAN interface is wan1, and the secondary WAN interface is wan2. These two interfaces will automatically get IP address using DHCP by default.
2. It is recommended that user backup the “startup-config.conf ” file first before upgrading firmware. The backup configuration file can be used if user wants to downgrade to an older firmware version.
3. If user upgrades from previous released firmware to this version, there is no need to restore to system default configuration.
4. After upgrade firmware, please remember to clear browser cache to avoid the GUI cache issue.
5. If it is difficult to configure via GUI (popup java script error, etc). It is recommended to logout the configuration window and clear browser cache first, then try to login and configure again.
6. To reset device to system default, user can press RESET button for 5 seconds and the device will reset itself to system default configuration then reboot automatically.
   - Note 1: After resetting, the original configuration will be removed. It is recommended to backup the configuration before performing this operation.
   - Note 2: After resetting, if user has subscribed to security licenses, user needs to connect to internet with myZyXEL.com and refresh license information.
7. If there is problem to reboot successfully after firmware upgrade, please refer to Appendix 3: Firmware Recovery.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

8. Since BWM has been activated in system default configuration, please remember to turn off BWM before you do the performance testing.

Design Limitations:

Note: These design limitations will be removed on next release once it is created into announced knowledge base.

Anti-Virus

1. [SPR: 070813118]
   [Symptom] ZyWALL has the limitation on concurrent sessions for ZIP and RAR decompression. If the limitation has been reached (typically in HTTP traffic), the event would be logged and the action depends on the checkbox (Destroy compressed files that could not be decompressed) is checked or not. If checked, compressed files would be destroyed, otherwise, bypassed.
   [Workaround] Unchecked the option of "Destroy compressed files that could not be decompressed" in the AV settings.
2. [SPR:100408336]
   [Symptom] DUT can't detect Virus if the compress file includes virus file and encryption file. And the encryption file is list as first in the compress file. This is our design issue that AV will ignore detection when encounter encryption file.
3. [SPR: 111027822]
   [Symptom] AV black/white list functionality abnormal with special HTTP URL(such as http://1.1.1.1/download/?command=download&filename=abc.zip)
   [WORKAROUND] Add wildcard rule "*abc.zip" to support this case

Build in Service

1. [SPR: 061208575]
   [Symptom] If users change port for built-in services (FTP/HTTP/SSH/TELNET) and the port conflicts with other service or internal service, the service might not be brought up successfully. The internal service ports include 10443/1723/2601-2604. Users should avoid using these internal ports for built-in services.
   [Workaround] Users should avoid using these internal ports for built-in services.
2. [SPR: 100419981]
   [Symptom]DNS doesn't resolve 2nd level domain name.
   Example:
   System-＞DNS-＞Address/PTR Record, add two record

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

a) testdomain.com 192.168.10.100
b) www.testdomain.com 192.168.10.100
DUT does NOT resolve the testdomain.com

Certificate

1. [SPR: 080509434]
   [Symptom] Cannot input L(locality name) & ST(state or province name) etc when create a certificate request.

EPS (Endpoint Security)

1. [SPR: 090805245]
   [Symptom] PC OS is 64 bits. EPS always fail when checking Firewall, Anti-virus and Windows auto update.
   We current not support EPS on Windows 64bit Operation System.

GUI

1. [SPR: 100415854]
   [Symptom] The GUI's initial help page's behavior was wrong. This owing three layer open web-help caused this.
2. [SPR: 100914249]
   [Symptom]IE7/8 sometimes shows "Stop running this script? A script on this page is causing Internet Explorer to run slowly. If it continues to run, your computer may become unresponsive." when configuring device. Please update IE patch: http://support.microsoft.com/kb/175500 for fixing this issue
3. IE7/8 sometimes shows "A script on this page is causing Internet Explorer to run slowly..." when configuring device. Please update IE patch : http://support.microsoft.com/kb/175500 for fixing this issue
4. [SPR: 101116922]
   [Symptom]GUI response will become very slow or hang sometimes. You can reopen the browser to solve this problem
5. [SPR: 110908044]
   [Symptom] Log-in with admin in Linux OS will fail in Opera 10.6x
6. [SPR: 110216901]
   [Symptom] When the admin logged in via web interface, the admin will be logged out by clicking the "refresh" button of the browser

Interface

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

1. [SPR: 100105242, 100105292] Since F/W version 2.12
   [Symptom] PPTP might not be able to connect successfully if it is configured via Installation Wizard/Quick Setup. This is because 1) Installation Wizard/Quick Setup only allows PPTP based interface to be configured with Static IP. 2) Installation Wizard/Quick Setup doesn't allow user to configure PPTP based interface's Gateway IP Address. This may caused PPTP cannot connect successfully if the PPTP Server IP is not at the same subnet with PPTP's based interface
   [Workaround]
   Before dial PPTP connection, configure the Gateway IP of PPTP interface's based interface

IPSec VPN

1. [SPR: 070814169]
   [Symptom] PKI does not interoperate with Windows CA server, when using SCEP.
2. [SPR: 070814168] Since F/W version 2.00
   [Symptom] VPN tunnel could not be established when 1) a non ZyWALL peer gateway reboot and 2) ZyWALL has a previous established Phase 1 with peer gateway, and the Phase 1 is not yet expired. Under those conditions, ZyWALL will continue to use the previous phase 1 SA to negotiate the Phase 2 SA. It would result in phase 2 negotiation to fail.
   [Workaround] User could disable and re-enable phase 1 rule in ZyWALL or turn on DPD function to resolve problem.
3. [SPR: 100429119] Since F/W version 2.11
   [Symptom] VPN tunnel might be established with incorrect VPN Gateway
   [Condition]
   1) Prepare 2 ZyWALL and reset to factory default configuration on both ZyWALLs
   2) On ZyWALL-A
      (1) Create 2 WAN interfaces and configure WAN1 as DHCP Client
      (2) Create 2 VPN Gateways. The "My Address" is configured as Interface type and select WAN1 and WAN2 respectively
      (3) Create 2 VPN Connections named VPN-A and VPN-B accordingly which bind on the VPN Gateways we just created
   3) On ZyWALL-B
      (1) Create one WAN interface
      (2) Create one VPN Gateway. The Primary Peer Gateway Address is configured as WAN1 IP address of ZyWALL-A and the Secondary Peer Gateway Address is configured as WAN2 IP address of ZyWALL-A
   4) Connect the VPN tunnel from ZyWALL-B to ZyWALL-A and we can see VPN-A is connected on ZyWALL-A
   5) Unplug WAN1 cable on ZyWALL-A

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

6) After DPD triggered on ZyWALL-B, the VPN Connection will be established again
7) On ZyWALL-A, VPN-A is connected. But actually ZyWALL-B should connect to VPN-B after step 5)

[Workaround] Change the WAN1 setting of ZyWALL-A to Static IP

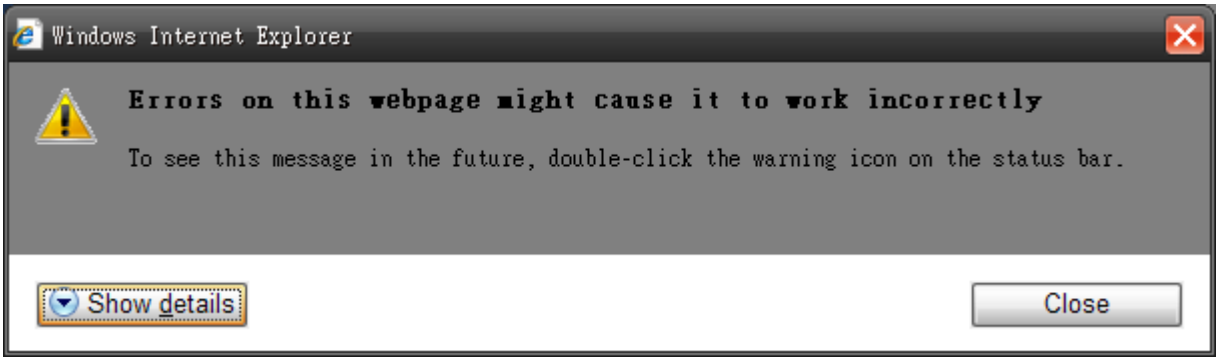
SSL VPN

1. [SPR: 091022383]
   [Symptom] SSLVPN cannot work anymore if below case is true
   1) Configure one SSLVPN policy and activate the Network Extension
   2) Add network A into Network List
   3) User login SSLVPN from network A
   4) The SSLVPN cannot be established and cannot work anymore

   [Workaround] Reboot DUT and remove network A from Network List.
2. [SPR: 091021328]
   [Symptom] SecuExtender agent cannot be launched in Windows Vista and Windows 7 If the "Computer Management/Services and Applications/Services/ZyWALL SecuExtender Helper" is disabled on user's computer before user tries to login SSLVPN.
   [Workaround] Enable ZyWALL SecuExtender Helper first before you try to login SSLVPN
3. [SPR: 090901070]
   [Symptom] Microsoft RDP Client Control may not work after user installs MS KB958469/958470/958471/956744. Using SSL VPN RDP function, after user install Remote Desktop Client Control (msrdp.cab), some PC may occur Javascript error.

Internet Explorer - Security Warning
Do you want to install this software?
Name: Remote Desktop ActiveX Control
Publisher: ZyXEL Communications Corporation
More options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.


Windows Internet Explorer
Errors on this webpage might cause it to work incorrectly
To see this message in the future, double-click the warning icon on the status bar.
Show details
Close

This problem caused by **MS KB958469/958470/958471/956744**. When user never uses RDP ActiveX control, and user install KB958469/958470/958471/956744, Windows will block the msrdp.cab installer.

KB offer matrix based on the RDC version and platforms

RDC versions (in-band and Microsoft-supported out-of-band releases)

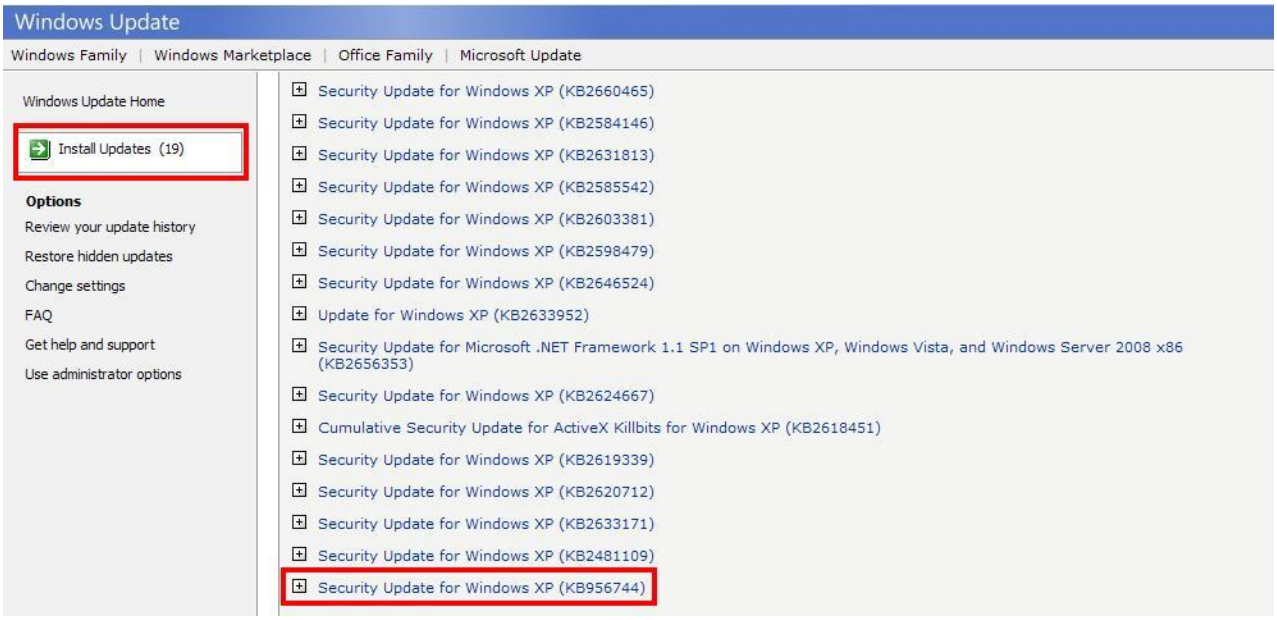
	RDC 5.0	RDC 5.1	RDC 5.2	RDC 6.0	RDC 6.1
Windows Vista RTM	x	x	x	KB956744*	x
Windows Vista SP1 and Windows Vista SP2	x	x	x	x	KB956744*
Windows XP SP2	x	KB958470*	KB958469	KB956744*	KB956744*
Windows XP SP3	x	x	KB958469	x	KB956744*
Windows Server 2003 SP2	x	x	KB958469*	KB956744*	x
Windows 2000 SP4	KB958471*	KB958470*	KB958470	x	x

Note In this table, x = not applicable.
Note In this table, almost all users are represented by the scenarios in the table that contain asterisks (*).

[Workaround]

To solve this problem, user can reinstall the KB958469/958470/958471/956744 after user failed to install msrdp.ocx. Go to Windows Update Site, the KB958469/958470/958471/956744 will reappear on the web site. To install the RDP function could be used.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.


Windows Update
Windows Family | Windows Marketplace | Office Family | Microsoft Update
Windows Update Home
Install Updates (19)
Options
Review your update history
Restore hidden updates
Change settings
FAQ
Get help and support
Use administrator options
Security Update for Windows XP (KB2660465)
Security Update for Windows XP (KB2584146)
Security Update for Windows XP (KB2631813)
Security Update for Windows XP (KB2585542)
Security Update for Windows XP (KB2603381)
Security Update for Windows XP (KB2598479)
Security Update for Windows XP (KB2646524)
Update for Windows XP (KB2633952)
Security Update for Microsoft .NET Framework 1.1 SP1 on Windows XP, Windows Vista, and Windows Server 2008 x86 (KB2656353)
Security Update for Windows XP (KB2624667)
Cumulative Security Update for ActiveX Killbits for Windows XP (KB2618451)
Security Update for Windows XP (KB2619339)
Security Update for Windows XP (KB2620712)
Security Update for Windows XP (KB2633171)
Security Update for Windows XP (KB2481109)
Security Update for Windows XP (KB956744)

More information can see Microsoft Support Site:

http://support.microsoft.com/kb/958469

http://support.microsoft.com/kb/958470

http://support.microsoft.com/kb/958471

http://support.microsoft.com/kb/956744

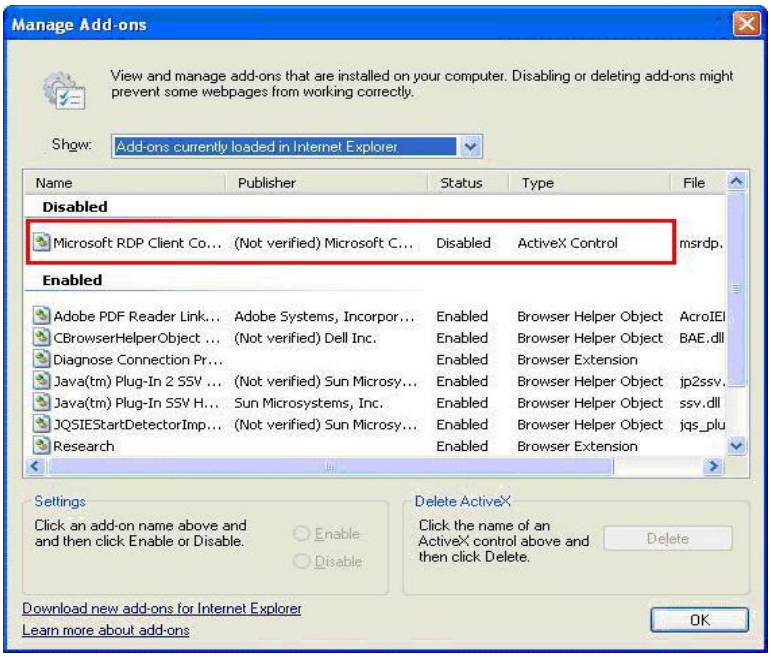
4. [SPR: 100413593]

[Symptom] Can not login remote RDP server via SSLVPN

Microsoft RDP Client Control may not work in IE7/IE8 after WinXP SP3

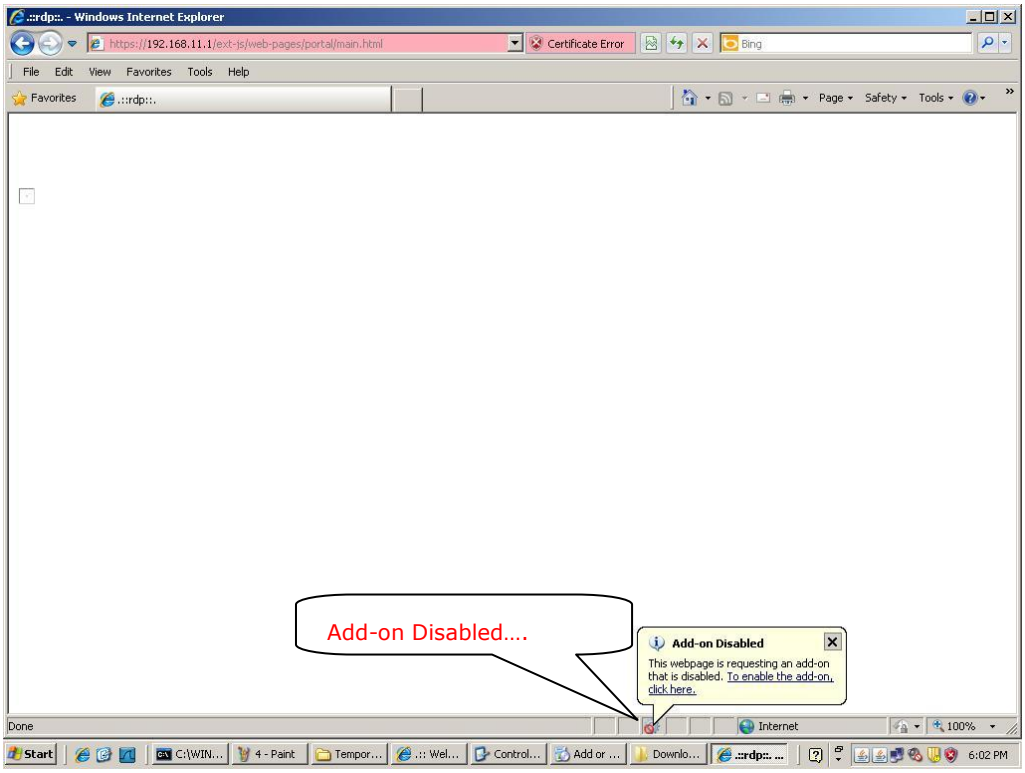
To use SSLVPN Portal RDP function, the web page must load the Microsoft RDP Client Control. This ActiveX control must be set to enable, or the function would not work. In IE6, we can find the option in [Tools→Manage Add-ons] and set the option to enable.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.



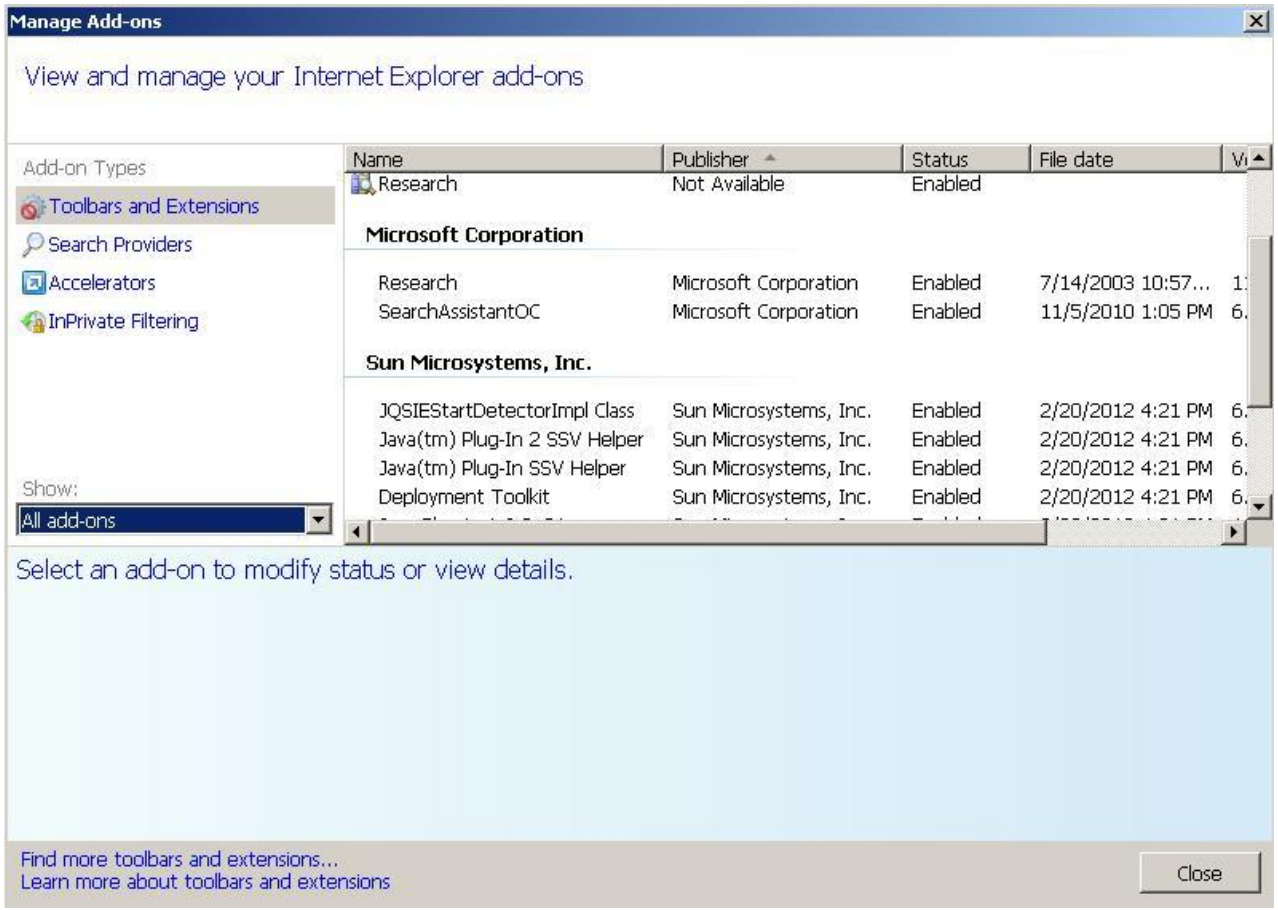
After WinXP SP3 Microsoft RDP Client Control is set disable as default value. If user never used the RDP control in IE6 and set to enable. After upgrade to IE7/IE8, user may get the message:

Add-on Disabled This Webpage is requesting an add-on that is disabled. To enable the add-on click here.



But when click the add-on, The RDP Client Control couldn't be found in Manage Add-ons.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.



[Solution]

Microsoft provides the solution to solve this problem in their official support website. User can follow the official to enable the RDP ActiveX control.

http://support.microsoft.com/kb/951607

1) Click Start, Run. Type Regedit.exe and press ENTER.
2) Remove the following registry key:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{9059f30f-4eb1-4bd2-9fdc-36f43a218f4a}

3) Restart Internet Explorer, and try to connect to the RDP application again.

For IE7 user may encounter browser always remind you to install related Active X; this owing to the security policy, you need set the value of Allow previously unused ActiveX controls to run without prompt to Enable. Please seethe following step:

a) From the **Tools** menu, click **Internet Options**.

b) On the **Security** tab, select the zone that contains the Web Interface server and click **Custom level**.

c) Set **Allow previously unused ActiveX controls to run without prompt** to **Enable**

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

5. [SPR: 080430468] Since F/W version 2.11 ➔ Design
   [Symptom] Cannot install SSL VPN RDP web component in Vista and WIN 2000
   [Workaround] Windows XP SP3/RDP 6.1 breaks RDP connection through Internet Explorer.
   Following is the SSL VPN RDP limitation table.

Applications Operating System	Full Tunnel Mode	Reverse Proxy Mode File Sharing(Web-based Application)	RDP	VNC
Windows 7 (X64) (SP1) JRE 1.6.x Java 7 -	Internet Explorer 8.x, 9.x Chrome latest version Firefox latest version Opera latest version Safari latest version	Internet Explorer 8.x, 9.x Chrome latest version Firefox latest version - Safari latest version	Internet Explorer 8.x, 9.x	Internet Explorer 8.x, 9.x Chrome latest version Firefox latest version - Safari latest version
Windows 7 (X32) (SP1) JRE 1.6.x Java 7 -	Internet Explorer 8.x, 9.x Chrome latest version Opera latest version Safari latest version	Internet Explorer 8.x, 9.x Chrome latest version Firefox latest version - Safari latest version	Internet Explorer 8.x, 9.x	Internet Explorer 8.x, 9.x Chrome latest version Firefox latest version - Safari latest version
Windows 8 (X64) Java 7	Internet Explorer 10.x Chrome latest version Firefox latest version Opera latest version Safari latest version	Internet Explorer 10.x Chrome latest version Firefox latest version Safari latest version	Internet Explorer 10.x	Internet Explorer 10.x Chrome latest version Firefox latest version Safari latest version
Windows 8 (X32) Java 7	Internet Explorer 10.x Chrome latest version Firefox latest version Opera latest version Safari latest version	Internet Explorer 10.x Chrome latest version Firefox latest version Safari latest version	Internet Explorer 10.x	Internet Explorer 10.x Chrome latest version Firefox latest version Safari latest version
Windows 2003 JRE 1.6 Java 7	Internet Explorer 7.0, 8.0 Firefox latest version	Internet Explorer 7.0, 8.0 Firefox latest version	Internet Explorer 7.0, 8.0	Internet Explorer 7.0, 8.0 Firefox latest version
Windows 2008 Java 7	Internet Explorer 8.0, 9.0 Firefox latest version	Internet Explorer 8.0, 9.0 Firefox latest version	Internet Explorer 8.0, 9.0	Internet Explorer 8.0, 9.0 Firefox latest version

6. [SPR: 100419034]
   [Symptom] SSLVPN of VNC cannot work if user connects VNC application by FQDN.
7. [SPR: 100427864]
   [Symptom] ActiveX cannot be installed successfully when using SSLVPN RDP function
   [Condition]

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

1) PC environment: Windows XP with SP3, using IE7 as browser.
2) Edit Object>SSL Application，add rules
   - Type=Web Application，Server Type=RDP，Name=RDP_Windows
3) Create one SSLVPN policy which selects the SSL Application we created
4) Login SSL VPN but can not open RDP_Windows portal by Full Screen and 32-bit color.
5) GUI will ask user to install terminal services ActiveX Client continuously

[Workaround]

This is because IE7 doesn't allow previously unused ActiveX controls running by default. We need to change the default behavior to allow ActiveX controls in IE7. See below procedures

1) Click Tools > Internet Options
2) Select Security tab
3) Select Internet Zone and click "Custom level"
4) Enable the ActiveX option "Allow previously unused ActiveX controls to run without prompt"

8. [SPR: 101125986]
   [Symptom] Cannot install SecExtender on IE x86 64-bit. [Solution] Use Java or 32-bit IE to install SecExtender
9. [SPR: 110509643]
   [Symptom] In SSL-VPN file sharing configure object page, if user tries to preview an unreachable file sharing site, you need to wait for GUI response about 3 ~ 5 minutes.
   [WORKAROUND] You can press refresh to cancel the preview action.
10. [Symptom] SSL-VPN file sharing not support NTLMv2 and SMBv2

L2TP VPN

1. [Symptom] L2TP connection will break sometimes with Android device. This issue comes from the L2TP Hollow packet will not by replied by Android system.

User Aware

1. [SPR: 070813119]
   [Symptom] Device supports authenticating user remotely by creating AAA method which includes AAA servers (LDAP/AD/Radius). If a user uses an account which exists in 2 AAA server and supplies correct password for the latter AAA server in AAA method, the authentication result depends on what the former AAA server is. If the former server is Radius, the authentication would be granted, otherwise, it would be rejected.
   [Workaround] Avoid having the same account in AAA servers within a method.

USB Storage

1. [SPR: 100708070]

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

[Symptom] When rename system name, the USB storage can not work.

IPv6

1. HTTP/HTTPS not support IPv6 link local address in IE7 and IE8.
2. Windows XP default MS-DOS FTP client cannot connection to device's FTP server via iPv6 link-local address.
3. [SPR: 110803280]
   [Symptom] Safari cannot log in web with HTTPS when using IPv6
4. [SPR: 110803293]
   [Symptom] Safari fails to redirect http to https when using IPv6
5. [SPR: 110803301]
   [Symptom] Safari with IPv6 http login when change web to System > WWW, it pop up a logout message. (HTTP redirect to HTTPS must enable)

App Patrol

1. [SPR: 110331977]
   [Symptom] To use AppPatrol to block IM(Yahoo/MSN) Video or Audio, it only take effect when enable blocking of both Video and Audio signature
2. [Symptom]
   Sometimes some BT sessions cannot be identified. Owing to 15 packets limitation. If definition packets come after 15 packets in front of payload, the session will be established. Also, the p2p connection type are polymorphic (even encrypted) and hard to identify all sessions
3. [SPR: 110901220/110901210]
   [Symptom] BWM cannot limit WangWang(SPR: 110901220), BT, Thunder(SPR: 110901210) traffic

Anti-Spam

1. [SPR: 110418626]
   [Symptom] Google DNS server (8.8.8.8) may not answer the DNSBL query.

Content Filter

1. [SPR: 111028006]
   [Symptom] In CF warning page, the button (exit) cannot work with warning body message in Firefox

   [Workaround] User can take following steps to solve this issue in Firefox.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

a) Open Firefox and input URL with “about:config”
b) Input “dom.allow_scripts_to_close_windows” as search condition and press enter
c) The filtered rule value is false. Double click it to turn it as true.

Known Issues:

Note: These known issues represent current release so far unfix issues. And we already plan to fix them on the future release.

Stability

1. [ITS: 59317]
   [Symptom] A user use his on-line backup File Server and when he starts download a lot of files (about 3.08GB), it always failed to download these files. The back-up server use HTTP protocol and java applet.
   [Workaround] Please contact CSO to get fixed date code.

IP MAC Binding

1. [ITS: 61185]
   [Symptom] There have no IP/MAC binding entry displayed in the IP/MAC binding table when many entries are configured.
   [Workaround] Please contact CSO to get fixed date code.

SSL VPN

1. [SPR: 110621773]
   [Symptom] Can not login SSL portal when using an external group user type account in Radius server.
2. [SPR: N/A]
   [Symptom] Windows 7 users cannot use SSL cipher suite selection as AES256.
   [Workaround] You can configure Windows cipher with following information
   http://support.microsoft.com/kb/980868/en-us

Auth Policy

1. [SPR: 110804598]
   [Symptom] When add an exceptional rule to pass TCP ports range 1024~65535 in force authentication, the client doesn’t need to login DUT and can open yahoo or other internet web

GUI

1. [SPR: 110512912]

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

[Symptom] When there are more than 10000 sessions in DUT, open session monitor page will caused GUI to return ”Device Error” message

EPS

1. [SPR: 120209992]
   [Symptom] EPS rule selects Avira Premium 2009 but use PC with Avira Premium 2010 can pass EPS checking
2. [SPR: 120209000]
   [Symptom] EPS rule selects Norton Internet Security 2011 but use PC with Norton Internet Security 2010 can pass EPS checking

IPv6

1. [SPR: 120214542]
   [Symptom] PC should no get DHCPv6 IP address from interface without VLAN Tag
2. [SPR: 120301132]
   [Symptom] IPv6 address sets up capital letter cannot be added.

IPSec VPN

1. [SPR: 120110586]

[Symptom] When set IPSec VPN with certificate and enable x.509 with LDAP, the VPN session must dial over two times and the session will connect successfully

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Features:

Modifications in 3.00(BDS.4)C0 – 2013/01/18

1. [ENHANCEMENT]
   Add UDP session time out setting on GUI, Firewall > Session Control page.
2. [ENHANCEMENT]
   GUI filter in Firewall (need to match “any” rule when choose “Zone”)
3. [ENHANCEMENT]
   PPTP throughput enhancement
4. [ENHANCEMENT]
   Allow static route to configure the default route 0.0.0.0
5. [ENHANCEMENT]
   Description:
   Update EPS signature file version 1.0.0.13
   The new EPS signature file adds signatures for the following new firewall and anti-virus software support.
   New Firewall software:
   McAfee_AntiVirus_Plus_2012
   McAfee_Internet_Security_2012
   McAfee_Total_Protection_2012
   Trend_Micro_Titanium_Internet_Security_2011
   Trend_Micro_Titanium_Maximum_Security_2011
   Avira_Internet_Security_2012
   Norton_Internet_Security_2012
   Norton_360_V6
   New Anti-Virus software:
   McAfee_AntiVirus_Plus_2012
   McAfee_Internet_Security_2012
   McAfee_Total_Protection_2012
   Trend_Micro_Titanium_Internet_Security_2011
   Trend_Micro_Titanium_AntiVirus_2011
   Trend_Micro_Titanium_Maximum_Security_2011
   Avira_AntiVirus_2012
   Avira_AntiVirus_Premium_2012
   Avira_Internet_Security_2012
   Norton_Internet_Security_2012
   Norton_AntiVirus_2012
   Norton_360_V6

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

ESET_NOD32_AntiVirus_5
Kaspersky Anti-Virus 7.x
Kaspersky Internet Security v7
F-Secure Anti_Virus 2010
F-Secure Anti_Virus 2011
F-Secure Anti-Virus Client Security v9
F-Secure Internet Security 2010
F-Secure Internet Security 2011
Microsoft Security Essentials
ESET smart Security 4
ESET smart Security 5
ESET NOD32 Antivirus v2.7
ESET NOD32 Antivirus v3
ESET NOD32 Antivirus v4
McAfee Antivirus Plus 2009
McAfee Internet Security 2009
McAfee Total Protection 2009
McAfee Antivirus Plus 2011
McAfee Internet Security 2011
McAfee Total Protection 2011

6. [FEATURE CHANGE] eITS#120301945
   WAS:
   After upgrade to 3.00 FW, "adjust-mss auto" not append old phase-I configure.
   IS:
   After upgrade to 3.00 FW, "adjust-mss auto" will append automatic.
7. [BUG FIX] SPR: 130110009
   Symptom:
   After rebooting,Tunnel Interface/Bridge/Virtual Interface IP can not save to 192.168.200.1
   Condition:
   1. VPN > SSL VPN > Global Setting, Network Extension Local IP = 10.10.10.1
   2. Interface > Tunnel, add a GRE tunnel
   - Interface Name = tunnel0
   - Zone = TUNNEL
   - Tunnel mode = GRE
   - IP Address = 192.168.200.1
   - Subnet Mask = 255.255.255.0
   - My Address = WAN1
   - Remote Gateway Address = x.x.x.x (WAN1 subnet’s IP)

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

3. Reboot device
4. After rebooting,Tunnel Interface/Bridge/Virtual Interface IP will save to 0.0.0.0
5. It should save to 192.168.200.1

8. [BUG FIX] eITS#120402918 , SPR: 120423709
   Symptom:
   The user is authenticated via AD server, and the username contains a spaces(eg. Rizhong Cheng). If the user tried to log in SSL VPN, it will be treated as a USG user.
   Condition:
   1. Running their windows AD as the AAA auth server for SSL vpn users.
   2. USG100 set an ext-user-group (zywallvpnusers) they have certain users on the AD who's usernames contain spaces eg Rizhong Cheng and some users that don't eg testuser.
   3. Since the upgrade from ZYWALL USG 100_2.20(AQQ.6)C0 to ZYWALL USG 100_3.00(AQQ.0)C0 when users with spaces in their names click on the SSL vpn login button they don't login to the SSL VPN, the zywall logs them into the USG as a user
9. [BUG FIX] eITS# 120403715 , SPR: 120510705
   Symptom: The Port Statistics Grid View show abnormal graphic
   Condition:
   1. Port Statistics Grid View show abnormal graphic.
      The Y-axis show maxinum 4000Mbps value.
10. [BUG FIX] eITS# 120502182 , SPR: 120524812
    Symptom: DDNS-Module shows missing IFace.
    When the words length over 15 characters, the DDNS will shown up the "p" character automatically.
    Condition:
    When the words length over 15 characters, the DDNS will shown up the "p" character automatically.
11. [BUG FIX] eITS# 120502681 , SPR: 120530183
    Symptom: USG 100 App patrol "MSN" use "From" criteria will causing policy inacitve
    Condition:
    MSN version:14.0.8117.416 / 15.4.3555.308
    Setting MSN rule (Forward, only block audio/vedio/file transfer)
    1. Setting detail policy block any source from "LAN1", MSN still can transfer files.
    2. Remove "From" criteria to any, only limit "Source" criteria, MSN will be block to tranfer files.
    3. Enable both from & source criteria, cleint still can transfer criteria.
    PS.You can only try add new MSN rule set "From" criteria and drop all traffic, the policy still can't work.
12. [BUG FIX] eITS# 120504065 , SPR: 120607420

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Symptom: Service Object abnormal delete

Condition:

1.) Create 3 Services Like A_1, A_2, A_2 with Port 81/82/83

2.) Create a Group A_Test and include A_1, A_2, A_3

3.) Create a Group Frank_Test and include any Service Port like AIM and the A_Test Group

4.) Create a Firewall Rule LAN1 to WAN all any just Service Frank_Tes Group

5.) Remove A_2 and A_3 from A_Tes Group

6.) Try to Delete A_2, device will show you can't delete it. But afterreboot device, I can delete A_2.

13. [BUG FIX] eITS# 120503134 , SPR: 120529109

Symptom: USG300 Bug2 l2TP using wrong Port for LDAP authentication

Condition:

Customer change LDAP port in server setting but they found device didn't work.

CSO operation.

They have let us check their verify steps and list for a SOP, we can see even customer change the port to other one, device still send to default port 389.

14. [BUG FIX] eITS# 120600203/ 120600344 , SPR: 120301945

Symptom: BWM rule set the outgoing interface to IPSec Tunnel has error.

Condition:

Two issue

1st:

1. Set up a BWM rule with outgoing interface set to IPSec tunnel.

2. check running config, the bwm rule outgoing interface subcommand is set to "trunk" not to "tunnel".

2nd:

1. Create a IPSec tunnel with IPSec policy name length over 16.

2. Set up a BWM rule with outgoing interface set to this IPSec tunnel. GUI shows error message.

15. [BUG FIX] eITS# 120503357/120707647 , SPR: 120615980

Symptom: Firewall rule doesn't work normally with empty object

Condition:

1- Create a empty Address group and a Address object 192.168.1.29 for test later.

2- Create a Firewall rule, condition is from lan to wan and select empty address group for source & action is deny.

3- Use a PC binding 192.168.1.29 ip address and ping 168.95.1.1 continually.

4- After add 192.168.1.29 object into empty address group, the PC's ping session doesn't block and open a new web page successfully.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

5- Inactivate the firewall and activate it, PC's ping session is blocked and can't open any web page.

6- According to step.4, pc can't access internet at this moment, but even remove 192.168.1.29 object from group, the PC also can't ping 168.95.1.1 and open web page successfully.

We need inactivate rule and activate it then let PC can access internet.

16. [BUG FIX] eITS# 120600858 , SPR: 120619153

Symptom:

USG-100 3G doesn't disconnect (After fallback to primary WAN, DNS query will still keep on passive WAN)

Condition:

1. In Network > Interface > Trunk, config a user configuration trunk.
2. Let wan1 as active mode, cellular as passive mode.
3. unplug wan1 link, the traffic will go through cellular interface.
4. replug wan1 link, the traffic will fallbak to wan1. But when capture the packet on cellular interface, it will has DNS query packet.

Note: DNS query should fallback to active interface(wan1).

17. [BUG FIX] eITS# 120404624, SPR: 120626580

Symptom: USG20. PPPoE is not up.

Condition:

It only occurs on customer enviroment.

1. In object, create isp account with "service name"
2. create ppp interface with isp account.
3. the customer can't bring up ppp interface.
4. by the packet capture -
   a. If user doesn't config "service name", server will not response PADO for device.
   b. If user config "service name", server will response PADO but device doesn't handle it.

18. [BUG FIX] eITS# 120600621, SPR: 120618066

Symptom: Receive mail from webmail site will not show complete subject

Condition:

Topology: webmail server<=WAN-DUT-Lan=> pc(receive mail)

1.Enable anti-spam

2.Send mail form the webmail site. Mail Subject is "Rendez-vous le 10 Juin chez Ford pour profiter doffres exce"

3. Receive the mail the subject was not complete. Subject show "Rendez-vous le 10 Juin chez Ford pour profiter d'offre"

19. [BUG FIX] eITS#120604140 , SPR: 120629820

Symptom: CF URL test failed.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Condition:

Customer found they can use URL test on Commtouch category but Bluecoat will fail.

20. [BUG FIX] eITS# 120303465, SPR: 120514996

Symptom: Probleem met 3.00 firmware

Condition:

With our USG 100/200/300 we have unfortunately a problem with the 3.00 firmware.

After upgrading all our USG's at our various offices located on different places. Unfortunately our Alcatel Access Points did not worked after the upgrade.

These Access Points must have a ipsec-nat-t (UDP 4500) session to build the WLAN controller to the headquarters.

Among these sites we have built several IPsec VPN tunnels for Internet connection.

This is what we have tried to determine the root cause of the problem:

- disable firewall
- disable content-filter/idp/adp/anti-virus
- Additional firewall allow rule with logging (We see no UDP4500 IPsec session pass through the firewall).
- Different MTU sizes in the IPsec VPN
- Test constructed sub-branch simulated with firmware 2.20 (AQQ.6) to 3.00 main branch does not work.
- The headquarters with the USG300 downgraded to 2.20 (AQE.6) to 3.00 sub location still did not work. Only when we have the USG on a sub location and the main fortress was downgraded to 2.20 v6 the Access Points worked again.

21. [BUG FIX] eITS# 120600591, SPR: 120607438

Symptom: clients can't use L2TP passthrough to internet after update to 300AQU0ITS-r32927

Condition:

Customer set a policy rout to control L2TP traffic pass through to internet, this setting is ok before 300AQU0ITS-r32742.bin but after upgrade to 300AQU0ITS-r32927.bin, it can't work.

22. [BUG FIX] eITS# 120603431, SPR: 120713977

Symptom: [E] USG-200 / L2TP LDAP

Condition:

After upgrade from 2.20 to 300AQU0ITS-r33404.bin, customer found they can't use LDAP user login to L2TP, local user still work.

CSO operation.

We have do a test and can reproduce it.

1. downgrade to 2.20
2. connect a LDAP and can build L2TP
3. upgrade to 300AQU0ITS-r33404.bin

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

4. build L2TP will have a login deny logs.(Incorrect Username or Password)
5. local user is fine.

23. [BUG FIX] eITS# 120600291, SPR: 120629859
    Symptom: USG-100 IPsec tunnel suddenly cannot be established anymore
    Condition:
    If using DDNS to build-up dynamic IPSec VPN, it will be successful in the beginning. After reboot, it will be failed because USG will use the wrong phase.
    The phase should be incoming_lan1, not studerus_lan.
    CSO operation.
    upload the customer's config and build-up IPSec VPN.
    a. Using IP address as my address, after rebooting, I still can rebuild VPN tunnel successfully.
    b. Using DDNS as my address, after rebooting, the VPN tunnel will be failed. I can reproduce the symptom.
24. [BUG FIX] eITS#120701745 , SPR: 120712820
    Symptom: After upload file to device, file_upload-cgi is dead.
    Condition:
    It can not be reproduce.
    After upload file to device, file_upload-cgi is dead.
    2 coredumps are attached.
25. [BUG FIX] eITS#120601715/120700429 , SPR: 120731283/120731284
    Symptom: USG 1000 Crash
    Condition:
    Thursday, June 07th the USG crashed, we move the last VPN's to USG-1000 and now we've 75 Tunnels on USG-1000.
    It's a mixed mode from Certificate and PSK Tunnels.
26. [BUG FIX] eITS# 120703349, SPR: 120703349
    Symptom: [E]USG series not accepting MS Windows ICS DHCP Lease
    Condition:
    usg20w --- lan cable --- laptop wired interface[LAPTOP] laptop WiFi interface --- Internet
    On laptop computer WiFi Interface is activated Internet Connection Sharing and use the wired interface to connect USG20W WAN interface.
    The result is USG 20w WAN interface connected to laptop wired interface is not acknowledging DHCP lease offer from Internet Connection Sharing server.
    When downgrade USG20W firmware to 2.21, it can get IP address from DHCP lease.
27. [BUG FIX] eITS#120701639 , SPR: 120701639
    Symptom:
    USG300: Content Filter will pop out error message. "System internal error. Invalid service"

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Condition:

Try to access Content Filter from WEB GUI. It will pop out an error message. 'System internal error. Invalid service.'

28. [BUG FIX] eITS# 120707485, SPR: 120808376

Symptom: L2TP can not build after device reboot.

Condition:

1. Set a PSK in L2TP GW like "12345678"
2. Connect to this L2TP with any Client try User: test Pass: 1234
3. Your connection is established now.
4. Reboot device
5. Try again L2TP connection, it will fail query with " Authentication failed" in Log
6. Inacticate this rule and activate this rule , L2TP works back to normal.

29. [BUG FIX] eITS#120700861 , SPR: 1208201051

Symptom: USG-1000 / L2TP User Auth will fail after 2 Weeks

Condition:

Customer setup L2TP on USG1000, but they found it can’t work after 14 days, reboot can’t resolve issue they have to inactive then active rule.

30. [BUG FIX] eITS#120707277

Symptom:

USG-300 / ZySH Daemon Issue, VPN can't build up and DSL disconnect Issue since Patch 4 Weekly

Condition:

Load customer's configuration, disable all the phase 2 VPN rules, zyshd hang.

31. [BUG FIX] eITS#120802215 , SPR: 120405276/120405277

Symptom: pro daemon dead after SSLVPN-Dial-in fail with FQDN

Condition:

(It can reproduced),OS Client=Win7,IE9.

1.Object>User/Group>User, add four local user "Test1", "Test2", "Test3" and "Test4".

2.Object>User/Group>Group, add two group "TestG1" and "TestG2", put Test3 into TestG1 and put Test4 into TestG2.

3.Object>SSL Application, add rules - Type=Web Application, Server Type=VNC, Name=RealVNC, Server Address(es)=LAN_SUBNET - Type=Web Application, Server Type=VNC,Name=TightVNC,Server Address(es)=LAN_SUBNET

4.VPN>SSL VPN>Access Privilege,add an access policy - Name=Test1_TestG1, Description=Test1_TestG1, User / Group Member=Test1, TestG1, Selected Application Objects=RealVNC - Name=Test2_TestG2, Description=Test2_TestG2, User / Group Member=Test2 TestG2, Selected Application Objects=TightVNC, UltraVNC

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

5.System>DNS, add a FQDN record(on Mx Record)- FQDN=vnc.hostpc1.com- IP Address=192.168.1.33

6.PC 192.168.1.33 on LAN side and enable VNC servers.

7.Test1 can login SSL VPN and only can see RealVNC on portal

8.Test1 can open RealVNC via portal to remote control server with FQDN (vnc.hostpc1.com) and check if click "Disconnect" and "Send Ctrl-Alt-Del" work

9.Check Log>View Log, there are Test1 and Test4 login SSLVPN log

10.Expect result: CLI can't show pro is pro daemon dead via portal.

11.Actual result: It can pop pro daemon dead and can't work success.VNC Server(PC)----LAN(DUT)WAN(10.1.4.x)----LAB----(10.1.4.x)SSLVPN Client(WIN7).

32. [BUG FIX] eITS# 120802538

Symptom:

After using IPSec/SSL VPN for a long time, the throughput drop and finally no more traffic can be encrypted/decrypted.

Condition:

1. This can be reproduced.
2. Using IPSec VPN for a long time, the throughput seems to be retricted and end up with 0 throughput.
3. Login with debug account and enter the command "cat /sys/module/ocf/parameters/crypto_q_cnt", you will see the value represents ocf queue length reaches to 1000.

33. [BUG FIX] eITS#120704432 , SPR: 120906390

Symptom: USG-1000 / 400 L2TP VPN’s after upgrade to v3.00 cause issue

Condition:

Before 2.20, customer found some of their L2TP can’t build with Cert not trusted logs, but after upgrade to 300BDQ0ITS-r33825.bin, all L2TP can’t build anymore.

CSO operation.

We have ask them provide config and diaginfo, but customer downgrade to 2.20 when they met the problem so diaginfo was collect at 2.20.

They will provide remote on Thursday(current schedule), we have ask them let us build L2TP to that device and provide teamviewer with console, so please let us know who will online help check this issue.

34. [BUG FIX] eITS# 120804388, SPR: 120904153

Symptom: Downloading large amount of emails outlook email dump fail

Condition:

1. Set outlook express sending HTML encode with base64.
2. Sending test mail by outlook express.
3. Resending this mail with multiple type attachement files.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

4. Receive this mail from Lan, device will generate oops.

35. [BUG FIX] eITS#120704432 , SPR: 120906390

Symptom: USG-1000 / 400 L2TP VPN's after upgrade to v3.00 cause issue

Condition:

Before 2.20, customer found some of their L2TP can't build with Cert not trusted logs, but after upgrade to 300BDQ0ITS-r33825.bin, all L2TP can't build anymore.

CSO operation.

We have ask them provide config and diaginfo, but customer downgrade to 2.20 when they met the problem so diaginfo was collect at 2.20.

They will provide remote on Thursday(current schedule), we have ask them let us build L2TP to that device and provide teamviewer with console, so please let us know who will online help check this issue.

36. [BUG FIX] eITS#120800870 , SPR: 120917060

Symptom: LAN1 will stop distributing IP once LAN2 is changed to DHCP Relay

Condition:

When LAN1 and LAN2 are both in the DHCP Server role, everything works fine. However, if the customer changes LAN2 to DHCP relay, LAN1 will stop answering DHCP requests from the PC in the LAN1 subnet. The DHCP lease time is very short, 1 min. As soon as the customer change LAN2 role back to the server role, LAN1 starts distributing IPs again.

Reproduce Step:

1. apply system default config.
2. pc on lan1 can get ip: 192.168.1.33
3. enter lan2 config, set static DHCP table, ip:2.2.2.2 MAC: AA:AA:AA:AA:AA:AA, apply it.
4. enter lan2 config, change server type to dhcp relay, apply it
5. pc on lan1 can not get ip.

37. [BUG FIX] eITS# 120803878

Symptom: USG1000 - Reboots automatically two times per day.

Condition:

1. This can't be easily reproduced.
2. In my surrounding, I can reproduced the issue and the reporduced step is:
   (1) Configure a Site-to-Site IPSec VPN rule with Enable Replay Detection.
   (2) Trigger dial.
   (3) Disconnect the tunnel.
   (4) Use CLI "debug ipsec crypto-layoff disable" to force software to encrypt/decrypt IPSec traffic.
   (5) Trigger dial.
   (6) Disconnect the tunnel.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

(7) Use CLI "debug ipsec crypto-layoff enable" to force hardware to encrypt/decrypt IPSec traffic.

(8) Modify VPN rule and uncheck the Enable Replay Detection.

(9) Trigger dial again and you will see kernel oops and then kernel panic.

38. [BUG FIX] eITS# 120901338

Symptom: L2TP TCP MSS adjustment does not work.

Condition:

L2TP TCP MSS adjustment does not work.

39. [BUG FIX] eITS#120804109 , SPR: 120925728

Symptom: L2TP Query DNS fail

Condition:

1. apply L2TP.
2. XP login L2TP
3. Use android mobile phone login L2TP.
4. XP use nslookup to result DNS can't success.

40. [BUG FIX] eITS#121000748 , SPR: 1210221657

Symptom: L2TP error log USG Send:[HASH][NOTIFY:INVALID_SPI]

Condition:

WinXP can’t connect to USG100 via L2TPoverIPSec ,but Win7 is OK.

The error log USG Send:[HASH][NOTIFY:INVALID_SPI]

CSO operation.

I can reproduce in my lab, please see the attached diaginfo, this is my test configuration file.

I use phase 1 :3DES SHA1/3DES MD5/DES SHA1 , phase 2:DES SHA1/3DES SHA1/ 3DES MD5 in this order, the result is Win7 ok, WinXP failed.

It will show log USG Send:[HASH][NOTIFY:INVALID_SPI], the customer would like to know , what does it mean?

When I change phase 2 in this order 3DES SHA1/3DES MD5/DES SHA1 , WinXP build successfully.

41. [BUG FIX] eITS#120602006

Symptom: Fax-machine using the SIP protocol does not work.

Condition:

Following is the customer's topology:

SIP-server - [Wan]USG[Lan] - VoIP-gateway - Fax-machine

The customer's symptom is:

1.When enable SIP ALG transformations function in SIP ALG, the phone all work fine, but fax stop work.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

2.When disable SIP ALG transformation function in SIP ALG, the fax work well, but the VOIP stop work.

42. [BUG FIX] eITS#121006856/121005323/120902676/121100647 , SPR: 121025068

Symptom: Usg1000 - L2TP-clients behind NAT

Condition:

2 clients behind the same NAT can't connect to the USG1000 by L2TP.

CSO operation.

I can reproduce in my lab. I tested two ways.

First, one is XP another one is Win7.

Second, two clients are Win7.

The result is the same, when first client connect successfully, another one will fail.

43. [BUG FIX] eITS#121003144, SPR: 1211221813

Symptom:

If the SIP ALG turn on, from [additional branch] to [branch] or [branch] to [branch], one-side hearing.

Condition:

pc-[branch usg20]-IPSec-[usg100]-IPSec-[branch usg20]-pc

If the SIP ALG turn on, from [additional branch] to [branch] or [branch] to [branch], one-side hearing.

44. [BUG FIX] eITS#121002120

Symptom: After device root, Sierra 305 cannot be detected.

Condition:

The customer using Sierra 305 to connecting the internet.

When plug-in the 3G card, the device work well.

But if reboot the device, then the device will not detected the 3G card.

45. [BUG FIX] eITS#121000722

Symptom:

When login as User on USG, get sometimes the message: \"You will be redirected to the login page due idle timeout or network problem.\"

Condition:

1. Enable auth policy, some PC still not login, and redirect non-request connect to device port 80.
2. This caused apache no resource to service User-aware page, page send interval check status will not response and pop message.

46. [BUG FIX] eITS#121100863 , SPR: 121115350

Symptom: USG-300 / Crash after 30 Minutes and no Login possible.

Condition:

1. Apply the attached conf file.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

2. disable all ipsec vpn rule, then pm daemon dead.

47. [BUG FIX] eITS#121103708/121200350 , SPR: 1212201565

Symptom:

Adding a policy route to allow L2TP to access the internet via USG; however, it will be failed. PPPoE is fine, but PPTP will be failed.

Condition:

PPTP server-----(WAN)USG A

|

PPTP ---- L2TP ---- PC

step1. USG A(DUT) dailed up to PPTP server and get an IP address

step2. PC then use this IP address to establish an L2TP conncection

step3. PC under WAN(105 network) can't establish L2TP connection with USG A

P.S: 3.00(BDQ.0)ITS-r33825 can establish L2TP connection successfully

3.00(BDQ.4)b3ITS-r33874 can not.

48. [BUG FIX] eITS# 121101600, SPR: 1211292214

Symptom: The monitor of users will show wrong IPs.

Condition:

Establish 3 more SSL or L2TP.Go to dashboard to show the users, it will appear wrong information. Please refer to the attachment.

49. [BUG FIX] eITS# 121101853, SPR: 121122835

Symptom: PC remove ZyWALL SecuExtender , PC will crash.

Condition:

1. It can be reproduce
2. PC OS is Windows 7 32bit
3. ZyWALL SecuExtender version is 2.5.17.0
4. PC remove ZyWALL SecuExtender , it will crash
5. PC can't remove ZyWALL SecuExtender
7. PC crash picture as attachment.ITS#121101853

50. [BUG FIX] eITS# 120500936, SPR: 120601030

Symptom: NAT Traversal reactive when reboot

Condition:

1. config isakmp policy without NAT-T in 2.20
2. After upgrade firmwar to 3.00 this policy will auto enable NAT-T

51. [BUG FIX] eITS#120404644, SPR: 120510697

Symptom: SMTP name enlarge from 30 -->60 (USG-50 / System Mail Log)

Condition: customer required the log setting > smt user Name length is not enough.

52. [BUG FIX] eITS# 120305907, SPR: 120516240

Symptom: TCP port 53 default is on (USG-100 / QNAP Virus)

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Condition:

Some internet environment client maybe link the (TCP port 53), check r23365 & r24360 the TCP port 53 default was disabled.

Need change the default tcp port 53 enabled, and disable by CLI command ”no ip dns server tcp-listen”.

53. [BUG FIX] ITS# 69872, SPR: 120605227

Symptom: IPSec VPN nailed-up Fail

Condition:

[Topology]

USG1(nail-up) <--------> USG2(no nail-up)

1、In USG1, configure a site-to-site vpn rule with nail-up and small phase 1 lifetime(300sec).

2、In USG2 configure a corresponding rule without nail-up.

3、Ping one packet to an inexistent PC under the USG2 local network to trigger DPD packet.

4、Wait for Phase 1 lifetime timeout and renegotiation a new phase 1.

5、Phase2 sa would be delete and can’t be triggered by nail-up.

54. [BUG FIX] eITS# 120500365, SPR: 120514994

Symptom: USG 100 - L2TP Authentication

The customer can’t establish the L2TP tunnel to device.

Condition:

CSO operation.

I have tried to create a new user and establishing the tunnel to the device.

After established the tunnel, the device deleted the tunnel immediately.

Also the log displaying the incorrect username or password(I have login the user page by that user).

So I collected the diag-info.

55. [BUG FIX] eITS# 120500691, SPR: 120509585

Symptom: System won’t redirect http to https if http server is not listen to port 80.

Condition:

System won’t redirect http to https if http server is not listen to port 80.

CSO operation.

Reproduce step:

1. Reset device to default
2. Disable firewall.
3. Configuration -> System -> WWW
4. Change http server port (for example:60000)
5. Try to access web GUI(for example: http://192.168.1.1:60000)

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Access fail

56. [BUG FIX] eITS# 120402403, SPR: 120509673

Symptom: Changing SSL VPN config will effect Zone setting.

Condition:

Customer found then they change SSL VPN setting, device will change Zone setting automatically.

CSO operation.

We can reproduce this issue, below are our steps,

1.create three SSL VPN rules and check all of them are import into SSL VPN Zone

2.change first SSL VPN rule, then we found this one is disappear in SSL VPN Zone

3.after that we back to SSL VPN rules, we found other SSL VPN ”Zone” setting become ”none”

57. [BUG FIX] eITS# 120500490/120501877, SPR: 120514995

Symptom: ZySH / Quick Sec Crash and all Tunnels disconnect

Condition:

After upgrade to ZLD 3.0, just 12/25 Tunnels can build up, when try change anything like set Rule inactive, ZySH / Quick Sec Crash and all Tunnels disconnect.

CSO operation.

We have give them RD’s suggestion with disable nail-up, please let us know when you will use DF to fix this issue.

Attachment are coredumps, diaginfo and config file.

58. [BUG FIX] eITS#120502879 , SPR: 120528999

Symptom: [E] USG-1000 / IP-SEC Modul

Condition:

Device will crash.Description.Customer use 04/30 ITS weekly FW and device crash again last week, look like ipsec daemon still have some problem, below they provide more info for us,USG-Crash, so all VPN´s down, after a while PSK VPN´s recovered successfully.Before Certificate VPN´s can established, we need reboot USG manually.

59. [BUG FIX] eITS# 120403394, SPR: 120528000

Symptom: USG300 - VPN Issue

Condition:

Can’t build-up IPSec site to site VPN if using certificate as authentication.Description.

If the customer used certificate as authentication, there will be no request sent out from USG.

But if he used pre-share key, the tunnel will send request out.CSO operation.

1. Upload the customer’s config and had a test. Unfortunately, I can’t reproduce the symptom.
2. Ask for remote access and try to build-up tunnel by certificate. But there was no request out even though I change the syslog level to debug.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

3. Change to pre-share key. I can see the logs.

60. [BUG FIX] eITS#120301945 , SPR: 120531292

Symptom: IPSec VPN adjust MSS does not work.

Condition:

Topology:

Client --- (LAN)USG1000(Ethernet) === IPSec VPN == (PPPoE)USG300(LAN) --- Server

1. Set up a IPSec VPN tunnel between USG1000 and USG300.
2. In USG300 VPN gateway setting, try set FQDN to peer gateway address.
3. IN USG300 IPsec rule setting, try set MSS adjustment to custom size to 1000.
4. Client use TCP connect to server through IPSec VPN tunnel.
5. Check the MSS size in the SYN/ACK packet at USG1000's LAN side, the value is not 1000.

61. [BUG FIX] eITS#120501305 , SPR: 120514003

Symptom: USG 300 reboots with coredump

Condition:

After config VPN, device will restart in 3-4 days and with a coredump.

CSO operation.

Now we are asking for their config file and topology, when we get these will try to reproduce check could we done that in short time.

62. [BUG FIX] eITS#120500936 , SPR: 120601030

Symptom: NAT-T will auto enable, after upgrade from 2.20 to 3.00

Condition:

1. config isakmp policy without NAT-T in 2.20
2. After upgrade firmwar to 3.00 this policy will auto enable NAT-T

63. [BUG FIX] eITS#120502982 , SPR: 120531281

Symptom: :[E] USG-100 Site to Site VPN and deactivate Tunnel Issue

Condition:

Customer found even they disable the L2TP phase2 rule, when remote device want to negotiation S2S VPN, it still try to use L2TP rule for default nego rule.

CSO operation.

We can reproduce this issue, these are our steps,

1.setup a S2S between A and B USG.

2.Enable nail-up on device A.

3.Inactive device B's L2TP rule.

4.Let S2S build up, then inactive S2S phase2 rule on device B directly.

5.In logs we can see device A try to nego device B's L2TP phase2.

6.Active device B's S2S phase2 then S2S become normal.

64. [BUG FIX] eITS#120400091, SPR: 120605200

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Symptom: VPNs Unstable

Condition:

The customer can establish L2PT tunnel successfully.

But if using continue ping to the PC that behind the USG around 1 hour.

Then the tunnel will been dropped, and the same IP unable established the tunnel any more.

Also using the other one IP address, can access to GUI, but can't login to the device.

Must reboot the device, the symptom will been improved.

CSO operation:

I have tried to reproducing this symptom in my lab, but the L2TP tunnel work fine.

This symptom just happened in the customer's site.

I test this with customer together, but since the symptom happened, I can't access the device any more.

And there without any core dump file.

65. [BUG FIX] eITS# 120504199, SPR: 120601009

Symptom: :[E] USG-1000 / Crash again and Certificate Tunnel can't recover

Condition:

Customer just Import a new Certificate, create a new VPN Tunnel / Replace old Certificate and delete old certificate, few minutes later, USG crash.

CSO operation.

We have check their diaginfo and found they use 3.00(AQV.0)-2012-05-23-120502879, we have ask them use this week's DF but front engineer told us this device can't reboot all the time, customer need wait for a confirmation with this week DF can resolve this issue or which DF can resolve this issue they will use it.

66. [BUG FIX] ITS#71626 SPR:120427049

Symptom: VLAN interface command saves at wrong CLI group id.

Condition:

1.Add a new VLAN interface with interace name as vlan3000.

2.Add a new PPP interface with interface name as testppp.

3. In CLI command mode, type "show running-config" to display current running-config.

4. We would see the save location of vlan3000 VLAN interface CLI is behind testppp PPP interface.

67. [BUG FIX] ITS#71484, SPR: 120306432

Symptom:

Connectivity check fail by using TCP when target is not in same subnet with the interface.

Condition:

1.

Internet-----(WAN1:59.124.163.155)USG-300(GE1:192.168.10.1)---(WAN2:192.168.10.34)USG-100

|

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

|-----(59.124.163.148)FTP server

2. USG-100 GUI -> Network -> Interface -> Ethernet -> WAN2 -> Enable Connectivity Check

*Check Method : tcp

*Check this address : 59.124.163.148

*Check Port : 21

Then you will see system log shows ”wan2 ping check is failed. Zone Forwarder removes DNS servers from records.”

68. [BUG FIX] ITS#71955, SPR:120312833

Symptom: Dynu dynamic dns service not working.

Condition:

1. Customer want to setup Dynu DDNS and will failed.
2. Set DDNS with Dynu Basic, but always update fail.

69. [BUG FIX] ITS#, 72033, SPR:120312812

Symptom: ZLD 3.0 / NAT-Traversal setting not saved to config file.

Condition:

1. Goto VPN > IPSec VPN > VPN Gateway.
2. Edit default rule and disable NAT Traversal.
3. Reboot the device, but the NAT Traversal will be re-enabled.

70. [BUG FIX] ITS#, 71954, SPR: 111011444

Symptom: Interface IP cannot modify anymore after using duplicate IP with SSL VPN IP.

Condition:

1. Can be reproduced.
2. Network> Interface> Ethernet, select one of Ethernet (ex. dmz) and modify IP Address = 192.168.200.1, IP Pool Start Address (Optional)= 192.168.200.33 then click to save it.
3. After pop up a warning message modify dmz’s IP Pool setting.
4. Expect result: dmz’s IP Pool Start Address can be modify with 192.168.3.33 and save without any warning message.Actual result: dmz’s IP Pool Start Address cannot modify and save success.

Please check attachment for video.

71. [BUG FIX] ITS# 72208, SPR: 120323975

Symptom: USG-100 L2TP password error after update to 3.0

Condition:

1. Create an user ”test” and password ”aaaa” in User object.
2. Upgrade firmware to ZLD 3.00.
3. Dial L2TP with PAP protocol will fail.

72. [BUG FIX] ITS# 120304686, SPR: 120419526

Symptom: Ping with a large size packet through IPSEC VPN tunnel will fail.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Condition:

Test topology:

PC------(LAN)DUT1(WAN)PPPoE=====IPSEC Tunnel====Ethernet(WAN)DUT2(LAN)

1. PC ping a large size packet to DUT2's LAN fail.
2. For example: ping LAN's IP -l 2000

73. [BUG FIX] ITS# 120304369, SPR: 120419524

Symptom: Duplicate domain zone in named.conf causes device fail to bring up named daemon.

Condition:

1. In System > DNS page, add some Address/PTR Record which has same domain name but with differenthostname.
   For example, test1.testdomain.tmp, test2.testdomain.tmp.
2. Sometimes, device will fail to bring up named daemon. Thus the DNS query go through device will fail to get a DNS replay.

74. [BUG FIX] ITS# 72194, SPR: 120406321

Symptom: ITS72194: USG-100 L2TP stress test leads to reboot

Condition:

Customer did stress test for L2TP

They build L2TP and disconnect continually.

Over ten times, a kernel crash was happened.

75. [BUG FIX] ITS# 71640, SPR: 120328442

Symptom: Apply ITS#71640 config of ZLD2.20 causes zyshd dead

Condition:

1. Apply the following commands or ZyDE_220p6.conf
   address-object Mailserver 192.168.111.5
   app other 1
   from WAN
   to LAN
   destination Mailserver
   bandwidth inbound 1000
   bandwidth outbound 1000
   log
   exit
2. Console shows zyshd dead.

76. [BUG FIX] ITS# 72417, SPR: 120330562

Symptom: After update 3.00 FW, Pre-Share key caused reboot device apply to default configure.

Condition:

1. Configure > VPN > IPSec VPN > VPN Gateway edit Default_L2TP_VPN_GW

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

2. Set Pre-Share key 1234 5678 wiht the space string.
3. After reboote devcie, configure apply to default configure.
4. Show error message. ERROR: isakmp policy Default_L2TP_VPN_GW encrypted-keystring $4$9l/e0dEE$MQS3HRJRmyhpQugUTKl5ccb5e6ODa7f13G2+dyH4VY+Mjh+GGt6rqymPcziOH1udbWzJkn/GaAF0kT/agO7EpriS1rEBYxLpxMvOo19jFnc$ 5678
Failed to apply startup-config.conf. Try to apply lastgood.conf or system-default.conf

77. [BUG FIX] ITS# 71847/eITS#:120401415, SPR: 120223596
Symptom: [Beta] Apply specific config file to device, it will take 40 minutes to finish it.
Condition:
1. Can be reproduced.
2. Apply the specific config file to device, it will take 40 minutes to finish it.
78. [BUG FIX] SPR:120418340
Symptom: DDNS couldn't auto update per 28 days
Condition:
79. [BUG FIX] eITS# 120204477, SPR:120327240
Symptom: BWM LAN to WAN UDP packet couldn't limit
Condition:
1. Set DDNS and it’s work normal.
2. But not auto update per 28 days period.
80. [BUG FIX] SPR:120322855
Symptom: L2TP and Auth. by ad-users does not work (BETA FORUM)
Condition: See attachment provided by beta user.
81. [BUG FIX] eITS# 120300323, SPR: 120327248
Symptom: Device registration loss and Anti-X disable.
Condition:
1. After update fw 00AQE0C0-2012-03-13#120300323.bin
2. Customer’s device will loss registration info on device and their anti-X will disable.
82. [BUG FIX] eITS# 120401998/120402803, SPR: 120426045
Symptom: HTTP throughput is slow with Commtouch content filter
Condition:
1. Enable content filter and use Commtouch service.
2. PC use www.speedtest.net to test HTTP throughout.
3. The test result is slow (only 10+ mbps with 50M line speed)
83. [BUG FIX] eITS# 120403778, SPR: 120426028
Symptom: [eITS#120403778]:[E] USG-300 / L2TP Payload Issue
Condition:

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

This one of the problem report on 120403246, in Phase 1 set: AES256, SHA1, DH1 then will cause L2TP have payload failed issue, customer has found a workaround change proposal can avoid this issue, but customer want a fix not a workaround.

CSO operation.

We have ask them provide their test steps,

1. USG with create two Policy, one L2TP Default just enable and one Dynamic Connection to IP Sec Client. In Phase 1 set: AES256, SHA1, DH1

2.Then connect with Android 4.X, IOS 5.1 or Windows 7. It will cause Payload Issue.

84. [BUG FIX] eITS# 120403270, SPR: 120426027

Symptom: [eITS#120403270]:[E] USG-20W / L2TP cause Daemon crash

Condition:

USG It seems Android query AES128 - SHA1 as first Payload, when this is not set, Daemon will crash, wrong Routing and PSK Error Message.After WORKAROUND: Change VPN GW IPSEC to SHA-512 it works fine.

CSO operation.

We will try to reproduce in local, attachments are the info customer provide, please check did these are as same as another issue.

85. [BUG FIX] eITS# 120304549, SPR: 120420627

Symptom: eITS#120304549:USG-1000 IPSec VPN Probleme Caritas

Condition:

Customer using PSK and certificate to build about 60-70 VPN tunnels(ZyWALL 2plus; USG Firewalls und ZyWALL2), there are many connection lost, In the GUI you can only see the tunnel is down,if they look on the Branch Office they see that the tunnel is build.

If they manually disconnect the tunnel and build than new the tunnel work.

CSO operation

We have ask them provide detail test steps,

1. Boot ok.
2. Tunnel buils susessfully
3. After ca. 2 - 5 min. all tunnels are shown as connected, - Also deactivated tunnels?!
4. The ZySH Wathcdog deamone restarts, ”Not connected to zysh daemon”
5. After short Time the Service is Running, but only VPN Tunnels with PSK are connected and not the important Certificates Tunnels!
6. Same effect after Reboot!

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Features:

Modifications in 3.00(BDS.2)b1 – 2012/04/27

1. [BUG FIX] ITS: 120401998, 120402803 SPR:120426045

   Symptom:

   HTTP throughput is slow with Commtouch content filter

   Condition:

   1) Enable content filter and use Commtouch service
   2) PC use www.speedtest.net to test HTTP throughput
   3) The test result is slow (only 10+ Mbps with 50M line speed)

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Features:

Modifications in 3.00(BDS.1)C0 – 2012/03/02

Modified for formal release.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Features:

Modifications in 3.00(BDS.1)b1 – 2012/02/22

1. [BUGFIX] SPR:120213426

   Symptom:

   ZyWALL 3.00 USG [coredumpApp] radiusd daemon dead!!

   Condition:

   4) Client uses OS : win7 SP1 32bit
   5) AAA server(AD,LDAP,RADIUS) OS: window 2003(AD server)10.1.7.33
   6) DUT setting please see attached conf.
   7) User alex belong testgroup in LDAP server can not use L2TP.
   8) User login L2TP, console display [coredumpApp] radiusd daemon dead message.
   9) Client setting :....->.... , enable Challenge Handshake & Microsoft CHAP v2
   10) Check 3.00b9 & 3.00b11 as the same problem.
   11) Please refer the attend file.Built-in service (HTTP/HTTPS, FTP, SSH, Telnet, SNMP), UAM, IPv6 log format support, DHCPv6, host, router, firewall, Interface and Transition Tunnel

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Features:

Modifications in 3.00(BDS.0)C0 – 2012/02/17

1. [ENHANCEMENT]
   IPv6 Support
   Built-in service (HTTP/HTTPS, FTP, SSH, Telnet, SNMP), UAM, IPv6 log format support, DHCPv6, host, router, firewall, Interface and Transition Tunnel
2. [ENHANCEMENT]
   Add CLI for showing IPv6 routing table
   CLI: show ipv6 route
3. [ENHANCEMENT]
   Add IPv4/IPv6 filtering in GUI interface edit page
4. [ENHANCEMENT]
   Add “renew” button for IPv6 interface in MONITOR>System status>Interface status>IPv6 interface status>Action field
5. [ENHANCEMENT]
   To accept user configure dhcpv6 lease object with request object for dns/sip/ntp server.
   Dhcpv6 lease object can configure "user defined" address or a request object which get value from dhcpv6 server.
6. [ENHANCEMENT]
   When upgrade FW form USG 2.2x or older version to USG3.0x, auto apply all ipv6 firewall rule for device
7. [ENHANCEMENT]
   DNS based inbound load balance
   1) Support ILB by modifying DNS response packets
8. [ENHANCEMENT]
   LB for inbound traffic
   1) Incoming traffic loading of each interface can be used as trunk load balancing criteria.
9. [ENHANCEMENT]
   Anti-Spam 2.0
   1) Query based
   2) Sender IP (IP Reputation)
   3) Add spam tag on X-header
   4) DNSBL enhancement: Only all query result said mail is white, the mail can be delivered. If it's black, take action immediately.
   5) Zero-day outbreak protection
10. [ENHANCEMENT]
    Add commands for AS ip reputation private check

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

CLI: [no] anti-spam ip-reputation private-check activate, show anti-spam ip-reputation private-check. The default action is “no”

11. [ENHANCEMENT]
    1) Add a commtouch/anti-spam graph to the Configuration>Licensing>Registration page.
    2) Insert an inote with "Anti-Spam Service helps your business network safe by blocking spam and harmful e-mails" to the Anti-Spam filed.
12. [ENHANCEMENT]
    AV White/Black list supports address object criterion.
13. [ENHANCEMENT]
    AV protocol configurable port
    1) Support HTTP/FTP/SMTP/POP3/IMAP4 configurable port
14. [ENHANCEMENT]
    AV SMTP virus notification (IMAP not support)
    1) Put warning string in the infected mail
15. [ENHANCEMENT]
    Add CLI command to enable/disable the mail infected message extension
16. [ENHANCEMENT]
    Trusted web-site increased from 32 to 100.
    1) Enlarge CF trusted web-site number
17. [ENHANCEMENT]
    CF white list can support wild card
    1) Support wildcard support in trust/forbid website and blocked URL keyword
18. [ENHANCEMENT]
    CF supports HTTP configurable port
19. [ENHANCEMENT]
    1) Add CF engine at present to the note field in Blocked web sites log, warning web sites log, forward web sites log.
    2) Add the information (Server ip, disable, elasped time, average time) to the CF debug log.
20. [ENHANCEMENT]
    Content filter daemon will pass those mimetype : gif, jpg, jpe, tif, png ,bmp, crl, css by default.
    We add three cli commands for usage :
    "content-filter mimetype ignore" --> default, ignore mimetype check
    "no content-filter mimetype ignore" --> check mimetype
    "show content-filter mimetype ignore status" --> show status
21. [ENHANCEMENT]
    Content-Filter Common Trust/Forbid List support
22. [ENHANCEMENT]

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Enable Commtouch and BlueCoat Security Threat (unsafe) categories when adding a new content filter profile

23. [ENHANCEMENT]

Reset content filter query server list daily (Default time: 3:07 am).

24. [ENHANCEMENT]

Support content filter display full URL path in debug log, including "Blocked Web Site", "Forward Web Site" and "Warning Web Site" log categories.

Prevent too many alert logs to send many emails.

1) Consolidate alerts to one mail

25. [ENHANCEMENT]

Many one-to-one over IPSec

1) Support many one-to-one over IPSec

26. [ENHANCEMENT]

Tunnel based MSS manually adjustment

1) In order to prevent packet fragmentation of IPSec packet, provide manual MSS configuration for each IPSec VPN tunnel

27. [ENHANCEMENT]

1) IPSec QuickSec4.4 SHA2 Support.
2) This Enhancement is to add SHA256 and SHA512 hash algo besides the existent MD5 and SHA1.
3) Either phase1 or phase2 are support SHA2 now.

Bellow is each product SHA2 SW/HW support list:

	HW Support **SHA256** with **non-null** encryption	HW Support **SHA512** with **non-null** encryption	HW Spec.	SW Support
USG20 USG20w USG50	**HW**	**HW**	SHA256 SHA512	SHA256 SHA512
USG100 USG200 USG300	**HW**	**SW**	SHA256 SHA512	SHA256 SHA512
USG1000 USG2000	**SW**	**SW**	SHA256 SHA512	SHA256 SHA512

28. [ENHANCEMENT]

1) IPSec VPN Configuration Provision Design.
2) Not Support AH active protocol.
3) Not Support for binding admin or limited-admin type user.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

4) Not Support IKE nego with certificate auth.
5) IPSec remote policy should be any, HOST type, or INTERFACE-IP type.

29. [ENHANCEMENT]
Support DHCP Relay over IPSec
30. [ENHANCEMENT]
QuickSec 4.4 certificate validation enhancement
31. [ENHANCEMENT]
VPN over Bridge
32. [ENHANCEMENT]
Client-Side VPN Failover Fallback Enhancement.
33. [ENHANCEMENT]
IPSec VPN support Configuration Provision Design.
34. [ENHANCEMENT]
1) Add i-note in all "zone combox"
2) Change all L2TP-IPSec VPN default zone from none to IPSec_VPN
3) Give a default zone for following interface/tunnel/VPN rule
a. GRE tunnel with TUNNEL zone
b. IPSec VPN with IPSec_VPN zone
c. L2TP VPN with IPSec_VPN zone
d. SSL_VPN with SSL_VPN zone
35. [ENHANCEMENT]
SSL VPN
1) SSL VPN support windows 2008 file sharing: User want to use SSL VPN portal's file link to integrate with Windows 2008 server
36. [ENHANCEMENT]
OWA exchange support
1) User need use proxy mode to support OWA exchange 2003, but not accept use full tunnel mode.
37. [ENHANCEMENT]
Upgrade SecuExtender from 2.5.12.0 to 2.5.13.0
a. New certification (expire date: 2013/04/07)
b. Client for support enforce all traffic by dut.
c. IE 64bit support
38. [ENHANCEMENT]
a. Upgrade SecuExtender from 2.5.14.0 to 2.5.15.0
b. Update new certification for jar file(expire date: 2014/02/17)
39. [ENHANCEMENT]
The SSL-VPN feature to force all client traffic into SSL VPN tunnel

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

40. [ENHANCEMENT]
    L2TP authentication over IPSec
    1) Support PAP/CHAP/MSCHAPv2/EAP-MSCHAPv2/EAP-PEAP(MSCHAPv2)
    2) Support Windows XP/Vista/7 and Apple iOS L2TP clients.
41. [ENHANCEMENT]
    1) L2TP over IPSec supports single sign-on (L2TP user aware).
    2) L2TP supports external group user.
42. [ENHANCEMENT]
    Max Session should be reserved for allowing GUI access
    1) Reserved some sessions for management use internal session number vs. external session
    2) ex. PM spec: 20000, actual 20200, but GUI should show 20000
43. [ENHANCEMENT]
    DNS support wildcard
    1) Support DNS wildcard in DNS records
44. [ENHANCEMENT]
    Auto-update certificate
    1) Device sync latest certificated from myZyXEL.com server
45. [ENHANCEMENT]
    USB storage support
    1) Store data (diagnostic info / log / crash dump / packet capture) to USB storage
46. [ENHANCEMENT]
    Enhance diag-info
    1) Collect diag-info when CPU/MEM reaches threshold.
47. [ENHANCEMENT]
    Enhance app-watch-dog
    1) Detect CPU/MEM usage high, dump the CPU info and memory usage of each process to the console.
48. [ENHANCEMENT]
    LDAP over SSL
    1) LDAP authentication between client and server can communicate through SSL.
49. [ENHANCEMENT]
    Support GRE tunnel
50. [ENHANCEMENT] ITS: 52490 SPR: 100823711
    TCP_in_window check need some log
    1) Add a log in debug log to let user know if his traffic is blocked by tcp_in_window check fail.
51. [ENHANCEMENT]
    GUI license promotion mechanism

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

52. [ENHANCEMENT]
    Dashboard information enrichment
    1) Top 5 firewall block rules
    2) Top 5 firewall6 block rules
    3) The latest alert logs
53. [ENHANCEMENT]
    SIP ALG enhancement to support multiple server in WAN and DMZ
54. [ENHANCEMENT]
    DHCP default gateway support in GUI
55. [ENHANCEMENT]
    Email logs add "date" field in mail header tag
56. [ENHANCEMENT]
    Support MAC OS in platform field for IDP signature
57. [ENHANCEMENT]
    Add trap for
        1) VPN tunnel disconnected
58. [ENHANCEMENT]
    Reseller information support
59. [ENHANCEMENT]
    Add 8 values supported for IP Precedence in "DSCP Code" and "DSCP Marking" columns
60. [ENHANCEMENT] ITS: 57707
    Add a switch "[no] arp reply restricted" to turn on and off the arp reply setting
61. [ENHANCEMENT] ITS: 58518
    Xauth and ISAKMP retry limit are too low.
62. [ENHANCEMENT]
    Support Static-Dynamic Route control One-One NAT.
63. [ENHANCEMENT]
    Policy routing criteria to support source port.
64. [ENHANCEMENT]
    Support application auto recover.
65. [ENHANCEMENT]
    PCI-DSS requirement 8.4 supported.
66. [ENHANCEMENT]
    Show well known port if the default port is unset for SMTP & POP3.
67. [ENHANCEMENT]
    Add CLI command to turn on/off apache compression function.
    Cli: [no] ip http content-compression.
68. [ENHANCEMENT]

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Add system default service objects: Kerberos-TCP, MS-RPC, LDAP-TCP, LPR, LDAPS-TCP, VNC5800, VNC5900, Kerberos-UDP, LDAP-UDP, LDAPS-UDP, L2TP-UDP, RADIUS-AUTH, RADIUS-ACCT, and BONJOUR.

69. [ENHANCEMENT]
    Support application watch dog perform system reboot
        a. Must defined compiler flag ZLDCONFIG_APP_AUTO_RECOVER
    b. Device reboot if recover fail more then 3 times.
    c. Device reboot directly when "Uamd" and "zyshd" dead/zombie.
70. [ENHANCEMENT]
    Update API: Service Refresh
    When do service refresh, send device's firmware version to MyZyXEL.
71. [ENHANCEMENT]
    Enable "Policy route overwrites 1-1 SNAT" automatically if enable "Static-dynamic route overwrites 1-1 SNAT"
    Close "Static-dynamic route overwrites 1-1 SNAT" automatically if close "Policy route overwrites 1-1 SNAT"
72. [ENHANCEMENT]
    Add information "user type" in "show users all".
73. [ENHANCEMENT]
    1) The fields of device selection will be hidden when insert 3G card has no support band feature.
    2) The fields of connection device show completely when mouse-over.
    3) Huawei E180 can work.
74. [ENHANCEMENT]
    Huawei EC1261 support (firmware:11.102.11.00.45)
75. [ENHANCEMENT]
    1) The fields of device selection will be hidden when insert 3G card has no support band feature.
    2) The fields of connection device show completely when mouse over.
    3) Support Huawei E180.
76. [ENHANCEMENT]
    Update EPS signature file from version 1.0.0.4 to version 1.0.0.9.
    New firewall software:
        Kaspersky_Internet_Security_v2011
        Kaspersky_Internet_Security_v2012
    New anti-virus software:
        Norton_Anti-Virus_2011
        Norton_Internet_Security_2011

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Norton_360_V4
Norton_360_V5
Kaspersky_Anti-Virus_2011
Kaspersky_Anti-Virus_2012
Kaspersky_Internet_Security_v2011
Kaspersky_Internet_Security_v2012
TrendMirco_PC-cillin_v2011_Cloud
Avira_Antivir_Personal_v2010
Avira_Antivir_Premium_v2009
Avira_Antivir_Premium_v10

77. [ENHANCEMENT]
    To change the state machine, try "Guest" account after anonymous login failed. If "Guest" can't login, prompt the login window for user input.
78. [ENHANCEMENT]
    AAA case-sensitive case-insensitive phase 1.
    a. Support case-sensitive and case-insensitive for Auth. Server (Radius, LDAP and AD).
    b. Default is case-sensitive.
79. [ENHANCEMENT]
    Support Huawei 3G generic driver architecture.
80. [ENHANCEMENT]
    VLAN/Bridge interface property support
81. [FEATURE CHANGE]
    WAS: Protocol name is case-sensitive in AppPatrol
    IS: Protocol name is case-insensitive in AppPatrol
82. [FEATURE CHANGE]
    WAS: The system default value of "tcp in window check" is not changed; we provide cli command for user to disable/enable
    IS: We set "tcp in window check" default value is disable
83. [FEATURE CHANGE]
    WAS: There was only EPS failure message in endpoint security
    IS: Add new EPS warning message options include “Windows Auto Update, Windows Security Patch, Firewall, Anti-Virus, Windows Registry, Application and File”
84. [FEATURE CHANGE]
    WAS: In a policy route rule with next hop is Trunk, and interface except passive interface are disconnect. When an interface is recover to alive, connections which outgoing is passive interface, will still alive.
    IS: (Fallback Session Disconnect)

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

In a policy route rule with next hop is Trunk, and interface except passive interface are disconnect. When an interface is recover to alive, connections which outgoing is passive interface, will forced to disconnect.

85. [FEATURE CHANGE]
Remove the function related GSB.

86. [FEATURE CHANGE]
WAS: Default value of content-filter zsb query on.
IS: Default value of content-filter zsb query off.

87. [FEATURE CHANGE]
WAS: ZLDSYSPARM_CF_TRUSTED_WEB_SITE_MAX_NUM 128
ZLDSYSPARM_CF_FORB_WEB_SITE_MAX_NUM 128
ZLDSYSPARM_CF_URL_KEYWORD_BLOCK_MAX_NUM 64
IS: ZLDSYSPARM_CF_TRUSTED_WEB_SITE_MAX_NUM 256
ZLDSYSPARM_CF_FORB_WEB_SITE_MAX_NUM 256
ZLDSYSPARM_CF_URL_KEYWORD_BLOCK_MAX_NUM 128

88. [FEATURE CHANGE]
WAS: content filter report service is active
IS: content filter report service is inactive

89. [FEATURE CHANGE]
WAS: The default setting of checking common-list for each CF profile is off.
IS: Change the default setting is on.

90. [FEATURE CHANGE]
WAS: SSL-VPN network list limitation is 4.
IS: SSL-VPN network list limitation is 8.

91. [FEATURE CHANGE]
Login SSLVPN with non any application redirect to portal page.

92. [FEATURE CHANGE]
WAS: The BWM global switch setting was displayed on Policy Route.
IS: Remove the BWM global switch setting from Policy Route.

93. [FEATURE CHANGE]
WAS: Default_L2TP_VPN_Connection is Site-to-site with Dynamic Peer.
IS: Default_L2TP_VPN_Connection is Remote Access (Server Role).

94. [FEATURE CHANGE]
WAS: Only accept WEP KEY prefixed with "0x".
IS: Accept WEP KEY prefixed with "0x" or "0X" or without prefix.

95. [FEATURE CHANGE]
WAS: The maximum value of MSS adjustment in IPSec is 1500 bytes.
IS: The maximum value of MSS adjustment in IPSec is 1460 bytes.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

96. [FEATURE CHANGE]
    WAS: NAT-T in IPSec VPN phase 1 is default off.
    IS: NAT-T in IPSec VPN phase 1 is default on.
97. [FEATURE CHANGE]
    WAS: Not support French
    IS: Support French
98. [FEATURE CHANGE]
    WAS: Email daily report and zylog has no date header
    IS: Email daily report and zylog has date header
99. [FEATURE CHANGE]
    BWM2.0 not support incoming/outgoing interface as virtual interface.
100. [FEATURE CHANGE]
    WAS: Block IPSec/SSL VPN intra-zone
    IS: No block IPSec/SSL VPN intra-zone
101. [FEATURE CHANGE] ITS: 53558, 66528
    WAS: DHCPDISCOVER Option(51) : IP Address Lease Time
    IS: Remove DHCPDISCOVER Option(51) : IP Address Lease Time
102. [FEATURE CHANGE]
    WAS: uamd daemon dead and zombie will not reboot system.
    IS: uamd daemon dead reboot system.
103. [FEATURE CHANGE]
    WAS: USG100/200/300/1000/2000 UDP default timeout is 9 seconds
    IS: USG100/200/300/1000/2000 UDP default timeout is 60 seconds
104. [FEATURE CHANGE]
    WAS: Anti-Virus Black/White List check cannot fully match
    IS: Anti-Virus support Black/White List check fully match
105. [FEATURE CHANGE]
    WAS:
        1. ZyXEL vendor ID: 809
        2. the value of ZyXEL Vendor attribute is "type=admin,lease-time=100,reauth-time=100"
    IS:
        1. ZyXEL vendor ID: 890
        2. type : vendor type 1,
          lease-time: vendor type 2,
          reauth-time: vendor type 3
106. [FEATURE CHANGE]
        WAS: ADP enable by default in all USG series.
        IS: ADP disable by default in USG 20/20w/50.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

107. [BUG FIX] ITS: 54390 SPR: 110119986

Symptom:

In Authentication configuration of VPN Gateway Pre-Shared key and Certificate can be chosen simultaneously

Condition:

1. Apply the system-default.conf
2. Configuration ＞ VPN ＞IPSec VPN＞ VPN Gateway, to add a only rule
3. In Authentication, choose Certificate and then choose Pre-Shared Key
4. The Certificate and Pre-Shared be chosen simultaneously as attached.

108. [BUG FIX] ITS: 42880 SPR:110119942

Symptom:

Can not build up a L2TP IPSec tunnel when the IPSec policy for L2TP is not in the first place.

Condition:

1. Delete the default L2TP IPSec policy in VPN Gateway and VPN Connection.
2. Configure a normal IPSec tunnel for site to site static VPN and disable the policy enforcement. The IPSec tunnel should be activated.
3. Configure an IPSec tunnel for L2TP. This policy will be in the second place.
4. Configure the L2TP VPN setting. Then build the L2TP VPN from PC to device, but fail

109. [BUG FIX] ITS: 56232 SPR:101105600

Symptom:

There is a typo error in IKE log.

Condition:

1. Create an IPsec VPN, and let the Pre-Shared Key of two sites different.
2. Connect the VPN tunnel, then enter into MONITOR/Log, there is typo errors exist in the IKE log "INVALD_PALOAD_TYPE". It should be ”INVALID_PAYLOAD_TYPE”

110. [BUG FIX] ITS: 54467 SPR:101026312

Symptom:

If the SSL VPN user index is not correct, the user login web page will redirect to access page.

Condition:

1. Create two ext-group-user type users test-a and test-b, the index of test-a is smaller than test-b, and they both contain a user ”justin”.
2. Configure a SSL VPN with test-b as the user.
3. Login the SSL VPN with user justin, but you will login the access page

111. [BUG FIX] ITS: 56220 SPR: 101126179

Symptom:

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

SPI:0x0 seq:0x0 no rule found

Condition:

User has 2 USG 20's and has a VPN connected between the two. The VPN's can connect and pass traffic, however when he tries to use telnet through the VPN tunnel to access a device on the opposite side, it fails and he sees "SPI:0x0 seq:0x0 no rule found" in the log.

112. [BUG FIX] ITS: 56520 SPR: 101126180

Symptom:

The VPN can't work correctly when use subnet object with mask 255.255.255.255 for VPN NAT.

Condition:

1. Create one site-to-site VPN, PC1---(LAN)USG200(WAN)==VPN==(WAN)USG300(LAN)---PC2.
2. In USG200, Create a subnet object with 32-bit mask (255.255.255.255), then use this object in Outbound Source NAT.
3. The VPN can be connected, but the traffic can't work correctly until you change the object to host type

113. [BUG FIX] ITS: 56439 SPR: 101129375

Symptom:

“RST ACK” can’t pass through VPN tunnel.

Condition:

Topology:

TELNET server-------(LAN)USG200(WAN)======VPN======(WAN)USG300(LAN)------PC

1. Setup a site-to-site VPN tunnel between USG200 and USG300
2. TELNET server is a ZyWALL 5 with a firewall rule to ‘Reject’ telnet traffic to itself.
3. When the PC tries to telnet access the TELNET server, you will see there is no ”RST ACK” packet captured on the PC site which means the ”RST ACK” can’t pass through the VPN tunnel

114. [BUG FIX] ITS: 56717 SPR: 110119000

Symptom:

USG as an ipsec server with site-to-site-with-dynamic-peer role, the gui show that it can't save the policy route with auto-destination.

Condition:

1. Build an ipsec setting, USG50 as the site-to-site-with-dynamic-peer role and USG300 as the site-to-site role.
2. Add a policy route in USG50, change the type to vpn-tunnel with the ipsec-setting in the next-hop form. It will show the radio box of "auto-destination"

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

3. Check the "auto-destination and then save. It will show the "auto-destination " off when you open the setting

115. [BUG FIX] ITS: 57068 SPR: 110111218

Symptom: If the sharing file on Mac is configured to force to enter user name and password to access, after the user login the USG with SSL VPN, the sharing file can't be accessed, there is no window pop up to ask for the username and password, but an error "[400]Directory Operation Failed".

Condition:

Topology:

Desktop PC ----- Internet ------- USG 100 ---------- MacBook Pro (10.5.8 OS): 192.168.1.34

a) The sharing file on Mac is configured to force to enter user name and password to access.
b) Login the USG with SSL VPN, the sharing file can't be accessed, there is no window pop up to ask for the username and password, but an error "[400]Directory Operation Failed".

116. [BUG FIX] ITS: 53462 SPR: 100923820

Symptom: User who builds SSL VPN to USG wants to access NAS by IPSec but failed

Condition:

a) Topology: USG(WAN)======VPN=====(WAN)ZyWALL 2 Plus(LAN)------NAS
b) Configure the SSL VPN File Sharing for NAS server.
c) Add a static route for NAS server, then USG can select the right source IP.
d) Add a policy route to direct the traffic from USG to the NAS server by tunnel.
e) PC can not access NAS by SSL VPN File Sharing.

117. [BUG FIX] ITS: 58459, 59827

Symptom:

sshipsecpm is dead.

Condition:

sshipsecpm is dead.

118. [BUG FIX] ITS: 67293 SPR: 110919138

Symptom: If the user is connected via L2TP VPN and enters a password incorrectly more than 5 times (the default setting), then USG block all accounts have access to create a L2TP VPN connection.

Condition:

a) GUI->VPN->IPSec VPN->Active Default_L2TP_VPN_Connection
   1.1 VPN Gateway : Remote Access(Server Role)
   1.2 Local policy : INTERFACE IP, 192.168.1.1
b) GUI->VPN->L2TP VPN->Enable L2TP Over IPSec
   2.1 VPN Connection : Default_L2TP_VPN_Connection

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

2.2 IP Address Pool: DMZ1_SUBNET

c) GUI->Object->User/Group-> Add one user

3.1 User Name:test

3.2 User Type:user

3.3 Password:1234

d) LAN1 PC keyin wrong passwod and login failed 5 times, then you can't login anymore even you keyin right password.

e) Router(config)# show lockout-users

As following information, you can see test has been blocked.

No. Username Tried From Lockout Time Remaining

==========

1 test console 00:29:55

119. [BUG FIX] ITS: 65663 SPR: 110721390

Symptom: Device will reboot when click GUI->MAINTAINANCE->Packet Flow Explore 3 times

Condition:

a) Reset device.

b) Create 200 IPsec VPN rules

c) Create 200 policy-route rules(for USG 1000)

d) Next Hop : IPsec VPN rules

e) Click GUI->MAINTAINANCE->Packet Flow Explore 3 times, device will hang then reboot.

120. [BUG FIX] ITS: 63517 SPR: 110610961

Symptom: This issue is with disappearing VLAN settings after reboot or switch off/on zywall USG 200

Condition:

a) Create a VLAN interface with 192.168.200.1. At this time the system will remind "This IP is used by SSL VPN".

b) Change "Network Extension Local IP" of SSL VPN to another.

c) Configure VLAN to 192.168.200.1 again, reboot device, when device boots up it will be 0.0.0.0.

d) Configure VLAN to another IP, this problem doesn't exist.

121. [BUG FIX] ITS: 65468 SPR: 110712687

Symptom: DNAT is configured in a VPN connection rule. Everything works fine. If user changes the VPN gateway connection?s name, the DNAT rule is disappear. DNAT does not work anymore.

Condition:

a) Create a VPN gateway named "test".

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

b) Create a VPN connection named "test", with a DNAT rule
c) Change the VPN connection's name from "test" to "test1", then you can see the DNAT rule is disappeared.

122. [BUG FIX] ITS: 57470 SPR: 110331914

Symptom: HTTP downloading file through VPN tunnel may fail when session include out of order packet

Condition:

a) Topology

PC ----- ZyWALL 35 ----VPN------USG300----- internet

b) Use attached configuration file. (ADP must enable at USG300)
c) User use browser to download firefox binary from Firfox web site via above topology
d) Downloading may fail when session include out of order packet

123. [BUG FIX] ITS: 53755 SPR: 100817270

Symptom:

The VPN can't be created correctly by VPN-wizard when Pre-Shared key contains reserved characters.

Condition:

1) CONFIGGURATION->Quick Setup, choose VPN Setup.
2) Using the Pre_Shared Key:1234&*S#@^ to set up the VPN.
3) After the Wizard finishes, there is no Phase2 (Network Connection) and the VPN Gateway has an empty PSK or sometimes the PSK is incomplete.

124. [BUG FIX] ITS: 53808 SPR: 100825943

Symptom:

Not all interface traffic statistic can be cleared when enable "Reset counters after sending report successfully" or click button "Reset All counters" in email daily report.

Condition:

1) CONFIGURATION->Log&Report->Email Daily Report, enable and set up it.
2) MONITOR->Traffic Statistics, enable collect statistics, choose one interface (for example wan2) which has traffic to show the traffic statistics.
3) In email daily report, click button "Reset All counters", check the traffic statistics, and found that just wan2's traffic statistics has been cleared, but other interface traffic statistics can't be cleared.

125. [BUG FIX] ITS 50642 SPR: 100705370, 100716786

Symptom:

After there is no traffic from 3G interface for a long time, the 3G card stays at get signal fail status.

Condition:

1) The 3G card is AC880, connect the 3G interface to ISP server.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

2) Unplug all the LAN side wired in the device to make there is no traffic pass 3G interface.
3) Wait for a long time about one night, the 3G interface stays at get signal fail status.

126. [BUG FIX] ITS: 51582 SPR: 100705336

Symptom:

Upgrade 2.12(AQQ.1) to 2.20(AQQ.1), the "Duration" of traffic log which shows in the VRPT server is always 0.

Condition:

1) PC1-----(Lan)USG100(Wan) --------Kiwi SYSLOG server (PC2)
2) Enter into "CONFIGURATION->Log&Report->Log Setting", and set the remote server's address: PC2's IP, Log Format:VRPT/Syslog, Active log: enable traffic log.
3) Setup the software "Kiwi Syslog Daemon", and start the syslog daemon.
4) From PC1 access a web or download files from ftp server in usg100 Wan side, and find that the "Duration" of traffic log which shows in the "Kiwi Syslog" is always 0.

127. [BUG FIX] ITS: 52133 SPR: 100705337

Symptom:

It allows to select two same type of server groups when configure an authentication method on GUI.

Condition:

1) Configure two different AD servers correctly.
2) Add these two ad servers in an authentication method.
3) The AD server which is in the second position of Authentication Method doesn't work.

128. [BUG FIX] ITS: 52439 SPR: 100721123

Symptom:

Disable snmp and then reboot, command "show snmp status" will show error message and GUI "System->SNMP" will always show "Loading".

Condition:

1) Enter into "System->SNMP", disable snmp.
2) Reboot device.
3) Command "show snmp status" will show error message, and GUI always show "Loading", but no error message.

129. [BUG FIX] ITS: 53509 SPR: 100804198

Symptom:

Change the name of "DNS" in Service Group will make device fallback to lastgood configuration after reboot.

Condition:

1) Change the name of "DNS" to "DNS_GROUP" with default configuration file.
2) Reboot USG.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

3) There will be an error messages "Fallback to lastgood configuration" on the console.

130. [BUG FIX] ITS: 52490 SPR: 100816131

Symptom:

DUT use IE connect web site megaupload can't download.

Condition:

1) Use system-default configuration.
2) When use IE8 to capture the file http://www.megaupload.com/?d=Y40H4FI7, file could not be downloaded.
3) This bug may not always reproduce, it may only happens on IE8 and slow PPPoE WAN.

131. [BUG FIX] ITS: 49264 SPR: 100707006

Symptom:

Device sends update to DDNS server although the IP address doesn't change.

Condition:

1) Configure a DDNS profile "Eurilio", set WAN1 as Primary Binding Addressand choose interface as IP Address.
2) Let this profile update successful.
3) Renew WAN1 and get the same IP, but we also find a log: "Update the profile Eurilio has succeeded. The IP address of FQDN endorse.gotdns.org has not changed.".
4) But in such case if IP doesn't change, this profile doesn't need update, and should show this log: "Update profile Eurilio has skipped due to same IP.".

132. [BUG FIX] ITS: 49591 SPR: 100619026

Symptom:

When user do PCI risk scan, some items failed.

Condition:

Customer uses a fee web site to scan USG200, that can't be reproduced locally. The test result as follow:

Protocol	Port	Program	Risk	Summar
TCP	8443	Pcsync-https	5	Synopsis : The remote service supports the use of weak SSL ciphers. Description : The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all. See also : http://www.openssl.org/docs/apps/ciphers .html Solution: Reconfigure the affected application if possible to avoid use of weak ciphers. Risk Factor: Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
TCP	844.	Pcsync-https	4	Synopsis : Debugging functions are enabled on

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

the remote web server.
Description : The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. See also : http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf http://www.apacheweek.com/issues/03-01-24 http://www.kb.cert.org/vuls/id/288308 http://www.kb.cert.org/vuls/id/867593 http://sunsolve.sun.com/search/document.do?assetkey=1-66-200942-1
Solution: Disable these methods. Refer to the plugin output for more information. Risk Factor: Medium / CVSS Base Score : 4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N) CVE : CVE-2003-1567, CVE-2004-2320, CVE-2010-0386 BID : 9506, 9561, 11604, 33374, 37995 Other references : OSVDB:877, OSVDB:3726, OSVDB:5648, OSVDB:50485

133. [BUG FIX] ITS: 52494 SPR: 100318654

Symptom:

Changing ’Default Authentication Timeout Settings’ of ext-group-user doesn’t work

Condition:

1. Go to User/Group---＞Settings, change the ’Default Authentication Timeout Settings’ of ext-group-user. Set Lease Time: 144; Re-authentication Time: 144.
2. Add a ext-group-user testad. Make sure users in group testad can login device successfully.
3. Check the Remain lease time and remain auth. time is still 1440 min.

By the way, when add a user as ext-group-user type. You can’t select Use Default Settings or Use Manual Settings for Authentication Timeout Settings in the page. This is different with other user type

134. [BUG FIX] ITS: 55529 SPR: 101101017

Symptom:

Enable Content Filter Category Service (Managed Web Pages: block), but it’s fail to block.

Condition:

1. USG -- L3 switch -- PC
2. USG is set as bridge mode. Enable CF function.
3. Access web site from PC,it’s fail to block any web site

135. [BUG FIX] ITS: 55079 SPR: 101011180

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Symptom:

Special ip format in Trusted Web Sites will cause CF rule apply error

Condition:

1. Add a CF profile, input 123-reg.co.uk into Trusted Web Sites list. Others are default.
2. Add a CF rule using this profile. Error message will be shown

136. [BUG FIX] ITS: 32331 SPR: 100827086

Symptom:

Contfltd is dead.

Condition:

1. Create two users, such as user1 "test" and user2 "test12345678901234567890123456 7", then put them in a group.
2. Add a content filter policy rule, the user item set as this group.
3. Login with user1, then access url and do not logout user1. Then open a new browser window and login with user2 at the same PC.
4. Logout user2 or wait for about one minute, content filter daemon will be dead.

137. [BUG FIX] ITS: 54353 SPR: 100907627

Symptom:

In WWW->Service Control, the USG-200 can't select address-group.

Condition:

1. CONFIGURATION->Object->Address->Address Group, create an address group.
2. CONFIGURATION->System->WWW->Service Control, add an admin service control rule, edit the address object, and found that the address-group can't be shown in drop-down box

138. [BUG FIX] ITS: 54278 SPR: 100910107

Symptom:

The user name and password of PPTP and PPPOE don't support some special characters.

Condition:

1. Go to Object>ISP Account, add ISP Account.
2. Can't type password with character '?' in password field

139. [BUG FIX] ITS: 53660 SPR: 100906505

Symptom:

AAA server can't accept '?' as password character both in GUI and CLI, and '\' is not in the acceptable character list prompt box but it can be accepted in fact.

Condition:

1. Enter into "Object->AAA Server->Active Directory".
2. Add a new rule, configure the password which contains '?', then there will show a warning "The value in the field is invalid. It cannot exceed 32 characters.
3. The valid characters are [0-9][a-z][A-Z][-(){}^`+/:!*#$@&=$.~%,|;-]".

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

4. Acceptable character list don't contain '\', but it can be accepted

140. [BUG FIX] ITS: 58713 SPR: 110127905

Symptom:

The Drop-down list is not in alphabetic order.

Condition:

When editing or creating new firewall rule, list of the objects which can be used is not in alphabetic order.

141. [BUG FIX] ITS: 53789 SPR: 101012349

Symptom:

When force logout an "ext-group-user" type user, the Auth.policy can't work normally.

Condition:

1. Set a group in AD server, and create a user "test" in this group.
2. Add an AD rule, and fill with neccessary setting.
3. Set the AAA method as "group AD".
4. Enable Auth.Policy, enable "Force User Authentication", and set "Source address" as "LAN_SUBNET". When lan pc access an URL, it will redirect to login page.
5. Login with an "ext-grop-user" type user, and then we can access url.
6. Force logout this user, then we can still access url

142. [BUG FIX] ITS: 56038 SPR: 101101063

Symptom:

In Address and Service Group, the available member list doesn't display in alphabetic order.

Condition:

1. Enter into Object->Address->Address Group, add or edit an Address Group Rule, the available member list doesn't display in alphabetic order. And there is same issue exists in Service Group.

143. [BUG FIX] ITS: 55639 SPR: 101103357

Symptom:

USG reboot automatically every 24 hours.

Condition:

1. Enable Anti-Virus feature, select LAN to WAN direction and HTTP protocol to scan for viruses.
2. Use LAN PC to send a HTTP POST request to WAN HTTP server, and there’s no any string after POST request.
3. USG will reboot or crash automatically at this time

144. [BUG FIX] ITS: 55541 SPR: 101102158

Symptom:

USG300 kernel crash due to reference NULL pointer skb.

Condition:

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

1. USG300 crashes regularly and can not be reproduced locally

145. [BUG FIX] ITS: 55572 SPR: 101102159

Symptom:

DDNS backup function doesn’t work by disable interface.

Condition:

1. Add a DDNS rule. Primary Binding Address: ge3 interface IP; Backup Binding Address: ge2 interface IP.
2. Disable ge3 interface (turn off the lamp)
3. The DDNS will always bind with ge3 interface IP.
4. It won’t change into ge2’s IP, until you manually select the rule then click update

146. [BUG FIX] ITS: 55787 SPR: 101103279

Symptom:

The Zysh daemon will be dead, when too many interfaces are configured as DHCP server.

Condition:

1. Add some VLAN interfaces (VLAN11 to VLAN55). From VLAN11 to VLAN47 are configured as DHCP server.
2. Enable the DHCP server for VLAN48, then the USG1000 can't be accessed

147. [BUG FIX] ITS: 53683 SPR: 100818439

Symptom:

On AD/LDAP edit page, it doesn't allow to type AD/LDAP domain with space in Base DN and Bind DN fields.

Condition:

1. Go to Object>AAA server, edit AD/LDAP server settings and set Bind DN and Base DN.
2. Can't type AD/LDAP domain with the space character

148. [BUG FIX] ITS: 56175 SPR: 101110159

Symptom:

For group identifier, character SPACE cannot be entered in Web GUI nor CLI.

Condition:

1. Configure the AD/LDAP/RADIUS server
2. Go to Configuration ＞ Object ＞ User/Group ＞ User ＞ Add
3. enter the user name filed with ”DHCP Users”, choose the user type as ext-group-user
4. enter the group identifier filed as ”DHCP Users”, then you will see the red warning message.

149. [BUG FIX] ITS: 57356 SPR: 101217563

Symptom:

When password of Bind DN the user configured in AD server contains character '&'. "Wrong AAA test command" will be shown when the user clicks the test button to test the user.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Condition:

1. Add an AAA server and fill in related setting.
2. The password of bind DN is setting with character '&'.
3. Click the button "test" to test user in "Configuration Validation".
4. It will pop-up "Wrong AAA test command".

150. [BUG FIX] ITS: 54866 SPR: 101011183

Symptom:

The virtual server can't work when disable the virtual server rule and then enable it.

Condition:

1. Create a address object of "INTERFACE IP" type named WAN_IP, and use DHCP server to get IP.
2. Use follow CLI create a virtual server rule:
   "ip virtual-server FTP_test interface wan1 original-ip WAN_IP map-to 192.168.1.40 map-type original-service FTP mapped-service FTP nat-loopback".
   The virtual server rule can't work and just rebooting the device can resolve it, but the problem will happen again if you disable the rule and then enable it

151. [BUG FIX] ITS: 57095 SPR: 101228204, 101228200

Symptom:

In Web GUI, add zone cannot achieve the maximum amount.

Condition:

1. Add more than 10 zones in Web GUI.
2. The page will pop an alert window which show the message” Items have reached the maximum number”

152. [BUG FIX] ITS: 59727 SPR: 110303459

Symptom:

USG Series External Group User Can Access Internet after Logout

Condition:

1. User login with ext-group user.
2. User logout or from the gui force log out.
3. Use ping to verify the connection to Internet or use browser (IE, Firefox, Chrome) to access Internet.
   When an external group user, (AD/LDAP/RADIUS) logout from a user-aware, it still can access Internet.

153. [BUG FIX] ITS: 60033 SPR: 110406245

Symptom:

The virtual interface packet capture does not dump in usb storage.

Condition:

1. Create virtual interface.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

2. Capture virtual interface in usb storage.
3. In usb storage does not have this file.

154. [BUG FIX] ITS: 59121 SPR: 110225002

Symptom:

The customer uses USB storage to collect the packet, when the file name of the captured packets is too long, the packet files can't be neither downloaded nor deleted.

Condition:

1. Configure a PPP interface named "aaaaaaaaaaa".
2. Active USB storage service.
3. Capture the packets on interface "aaaaaaaaaaa", save the data to USB storage and set the file suffix as "-packet-capture".
4. The name of the captured file is "aaaaaaaaaaa--packet-capture00-2011-02-10T032651.00"

155. [BUG FIX] ITS: 61849 SPR: 110412946

Symptom:

Httpd security hold: Limited-Admin issue

Condition:

1. For upload file, browser will pop up error message.
2. For download file, device will send file with zero size.

156. [BUG FIX] ITS: 59967 SPR: 110304603

Symptom:

User's password is shown as plain text in debug logs.

Condition:

1. Add a normal user test with passwd 1234, and set user debug log setting "all"
2. Login user test.
3. The log of user debug will show "Auth User(test) pwd(1234) result()."

157. [BUG FIX] ITS: 62189 SPR: 110421920

Symptom:

ISP account password will be cut to 6 characters after edit the object again.

Condition:

1. In Object > ISP account, edit GE1_PPPoE_ACCOUNT
Username = test, password = 1234567890, then apply it.
2. Edit GE1_PPPoE_ACCOUNT again without change anything and apply it.
The password will be cut to 6 characters.

158. [BUG FIX] ITS: 70806 SPR: 120130392

Symptom:

Huawei E156G can't work on USG.

Condition:

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Insert E156G to USG then device can't detect the 3G card. Ping 168.95.1.1. Then you can't login device anymore and will see coredump in GUI after rebooting.

159. [BUG FIX] ITS: 68840 SPR: 111128817

Symptom: UAM daemon dead

Condition:

a) Config AD server
b) Add an ext-group user with AD server
c) Enable user idle detection
d) Lan PC login device with ext-group user
e) Ping 168.95.1.1. Then you can't login device anymore and will see coredump in GUI after rebooting.

160. [BUG FIX] ITS: 56405 SPR: 101229310

Symptom: Use SNMP tool scan USG WAN 161 port with high frequency will cause system hang sometimes

Condition:

a) Enable USG SNMP function.
b) Send a SNMP request from an unreachable port of WAN PC to USG WAN 161 port with high frequency, sometimes USG will hang.

161. [BUG FIX] ITS: 56675 SPR: 101223956

Symptom: If two L2TP clients behind one NAT router, the second L2TP client will take more than 30s to establish the IPSec connection

Condition:

Topology:

PC1 and PC2 --- NAT Router------USG 300 ----LAN

a) Enable "Use Policy Route to Override Direct Route" in policy route.
b) PC1 dials L2TP tunnel to USG300.
c) After the first connection established successfully, it will take more than 30 seconds for the second L2TP client PC2 to establish the IPSec connection.

162. [BUG FIX] ITS: 57332, 57357 SPR: 110103024

Symptom: Port Settings Ignore ?

Condition:

a) Router(config)# port status Port5
b) Router(config-port-status)# speed 10
c) Router(config-port-status)# exit
d) Router(config)# show port status. Then you will see port5 status is still 1000M/Full?

163. [BUG FIX] ITS: 56512 SPR: 101118302

Symptom: Zyshd dead when SNMP agent use SNMP_ZYSH executed to query MIB information about CPU usage

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Condition: When device turns on SNMP service, then SNMP agent want to get CPU usage. It is possible that the CPU usage equation is divided by zero.

164. [BUG FIX] ITS: 50497 SPR: 100608525

Symptom: SNMP manager can't show SNMP trap message when SNMP agent set trap message to version 1

Condition:

a) SNMP agent --- USG100(NAT) --- SNMP manager.
b) Set SNMP agent trap message to version 1, destination as SNMP manger IP, and destination port as 162.
c) Do some operations to generate trap message, such as make one port of SNMP agent up and down. SNMP manger can't accept trap message.

165. [BUG FIX] ITS: 61671 SPR: 110414272

Symptom: To configure PPP bind bridge then reboot DUT, you will see apply startup-config. Conf unsuccessfully and rollback to apply lastgood.conf

Condition:

a) To configure bridge interface br0.
b) To configure PPP interface Base Interface : br0
c) To reboot DUT. Then you will see apply startup-config. Conf unsuccessfully and rollback to apply lastgood.conf

166. [BUG FIX] ITS: 61038 SPR: 110401186

Symptom: There's a port forwarding rule in NAT Route, forward 2400 port to 443 port of USG100's WAN interface. Customer wishes to drop ZyWALL management (login GUI as administrator via https) from WAN zone, so he add a deny rule for WAN zone in Admin Service Control. But it doesn't work. He still can login device by https:// NAT Route IP:2400 from wan PC.

Condition:

a) In USG100, add a deny rule for WAN zone in Admin Service Control in [System -> WWW].
b) Add a NAT rule in other device forward 2400 port to 443 port into USG100's WAN interface.
c) PC from internet access https:// NAT Route IP: 2400, it will not be denied.

167. [BUG FIX] ITS: 59239 SPR ID:110223640

Symptom: PPPoE connection can’t be dialed up if service name is necessary.

Condition:

a) Set Service Name=test
b) From packet, you can see Service Name information is ignored by device

168. [BUG FIX] ITS: 66828 SPR: 110913515

Symptom: USB still save debug logs even if disable system debug logs.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Condition:

a) GUI-> CONFIGURATION-> Log & Report-> Log Setting-> Selection-> enable normal logs
b) Active USB
c) GUI-> Diagnostics-> System Log->Download file. You will see a lot of debug logs but only enable normal logs.

169. [UG FIX] ITS: 59327 SPR: 110301053

Symptom: It always failed to send mail successfully after changing password in System Log E-mail Server ½

Condition:

a) Click GUI->CLI window
b) Configure GUI->CONFIGURATION->Log & Report->Log Setting->System Log->E-mail Server 1
   b.1 User Name: aaa
   b.2 Password: 1234
c) You can see "logging mail 1 authentication username aaa password 1234" from cli window
d) Edit System Log->E-mail Server 1. The Password: 5678
e) You can't see "logging mail 1 authentication username aaa password 5678" from cli window

170. [BUG FIX] ITS: 65965 SPR: 110818044

Symptom: In device, ip/mac binding with static ip can't show host name

Condition:

a) GUI->CONFIGURATION->Network->IP/MAC Binding
b) Edit lan1
   b.1 Enable IP/MAC Binding
   b.2 Add one static dhcp bindings rule
      b.2.1 IP Addrerss : 192.168.1.50
      b.2.2 MAC Address : according to yourself PC
c) PC plug into lan1

Then you will see Host Name is none in GUI->MONITOR->System Status->IP/MAC Binding

171. [BUG FIX] ITS: 65432 SPR: 110802099

Symptom: DUT will show cpu high when user set wan interface as dynamic ip

Condition:

a) Setup a dhcp server (Using pc or other machine) and edit the config to set five records of DNS servers.
b) Using the DUT wan interface as a dynamic ip.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

c) Set DUT LAN1 as a dhcp server, and first DNS server as wan1 1st DNS server, second DNS server as wan1 2nd DNS server,third DNS server as wan1 3rd DNS server.
d) DUT will show cpu hing after a moment.

172. [BUG FIX] ITS: 66147 SPR: 110805779

Symptom: Ftp port number is incorrect when enter debug mode.

Condition:

a) Reboot DUT(for USG 20)
b) Press any key to enter debug mode
c) “atkz -f -l 192.168.1.1” “atgo”
d) Then you will see ”Connect a computer to port 4 and FTP to 192.168.1.1 to upload the new file.” but only port 5 is active and can be upload file.

173. [BUG FIX] ITS: 64932 SPR: 110627184

Symptom: USG50 is not connected to pptp-server, but Win7 is OK.

Condition:

a) In ISP Account Rule
b) Set PPTP with Auth Type MS CHAP v2
c) Set Encryption Method MPPE 128 (encryption required)
d) Compression is ON

174. [BUG FIX] ITS: 64175 SPR: 110627227

Symptom: Login with ext-group-user account and DUT will hang over 5 mins

Condition:

a) Load the conf from customer.
b) Modify the config with test AD server and test account / group id.
c) Login with test account, the page will suspend with 5 mins because the weblogin.cgi cause the memory overwrite.

175. [BUG FIX] ITS: 63200 SPR: 110526349

Symptom: In the 2.12 firmware, the USG does not allow virtual server rules to be created when original IP is set to any and NAT loopback is enabled. When trying to create a similar virtual server rule in a USG with 2.20 firmware, the USG will warn the user saying that original IP is set to any while NAT loopback is enabled. However, the virtual server rule will be created. The light bulb of this virtual server rule is also yellow. But the virtual server rule will not work.

Condition:

a) In [Network -> NAT] add a rule.
b) Configure the following setting: Classification: virtual Server, Original IP: any, enable NAT loopback.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

c) Enter OK, it will show warning message like "Original IP cannot be set to ANY while NAT-Loopback is activated because it might cause device unreachable" and the rule can be establish.

d) User PC to connect to the server below the device will fail.

176. [BUG FIX] ITS: 61671 SPR: 110624073

Symptom: After applying system-default.conf then "Setup Wizard" page can't be brought up.

Condition:

After applying system-default.conf then "Setup Wizard" page can't be brought up.

177. [BUG FIX] ITS: 60820 SPR: 110329513

Symptom: USG send port traffic information to VRPT even if that port is down

Condition:

a) Configure VRPT server and USG300.

b) Cnnect the PC to USG300 Lan port 3, try to download 2 file(i??300M) from a ftp or web server.

c) After download it, disconnect the cable to the USG300.

d) You can see at this time the VRPT still shows traffic information of port 3 even if port 3 is down.

178. [BUG FIX] ITS: 61671 SPR: 110414272

Symptom: To configure PPP bind bridge then reboot DUT, you will see apply startup-config.conf unsuccessfully and rollback to apply lastgood.conf

Condition:

a) To configure bridge interface br0.

b) To configure PPP interface, Base Interface : br0

c) To reboot DUT

Then you will see apply startup-config.conf unsuccessfully and rollback to apply lastgood.conf

179. [BUG FIX] ITS: 61520 SPR: 110425226

Symptom: The customer has configured two PPPoE connection with nail-up. But when YTK-ppp connection drops, it can be reestablished manually (click the "connect" button on the Web GUI), but fails to be connected automatically, though nail-up is active.

Condition:

The customer has configured two PPPoE connection with nail-up. But when YTK-ppp connection drops, it can be reestablished manually (click the "connect" button on the Web GUI), but fails to be connected automatically, though nail-up is active.

180. [BUG FIX] ITS 59317 SPR: 110510739

Symptom:

When downloads a lot of files, with a total amount of 3.08GB, the USG eventually drops the file download. The time varies between 2-18 minutes. The amount of total size

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

downloaded spreads wide between 100Mbyte to 1.2Gbyte. The backup-applet uses HTTPS as protocol.

Condition:

1) If both ADP and IDP are disabled, everything works fine. But if one of them is enabled, it times out.
2) ZyWALL 2 Plus and ZyWALL 70 do not have this issue.
   This issue can only be reproduced by downloading from customer's server.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Appendix 1. Firmware upgrade / downgrade procedure

The following is the firmware **upgrade** procedure:

1. If user did not backup the configuration file before firmware upgrade, please follow the procedures below:
   - Use Browser to login into ZyWALL as administrator.
   - Click Maintenance > File Manager > Configuration File to open the Configuration File screen. Use the Configuration File screen to backup current configuration file.
   - Find firmware at www.zyxel.com in a file that (usually) uses the system model name with the .bin extension, for example, "300BDS0C0.bin".
   - Click Maintenance > File Manager > Firmware Package to open the Firmware Package screen. Browser to the location of firmware package and then click Upload. The ZyWALL automatically reboots after a successful upload.
   - After several minutes, the system is successfully upgraded to newest version.

The following is the firmware **downgrade** procedure:

1. If user has already backup the configuration file before firmware upgrade, please follow the procedures below:
   - Use Console/Telnet /SSH to login into ZyWALL.
   - Router>**enable**
   - Router#**configure terminal**
   - Router(config)#**setenv-startup stop-on-error off**
   - Router(config)#**write**
   - Load the older firmware to ZyWALL using standard firmware upload procedure.
   - After system uploads and boot-up successfully, login into ZyWALL via GUI.
   - Go to GUI → "File Manager" menu, select the backup configuration filename, for example, statup-config-backup.conf and press "Apply" button.
   - After several minutes, the system is successfully downgraded to older version.

2. If user did not backup the configuration file before firmware upgrade, please follow the procedures below:
   1. Use Console/Telnet /SSH to login into ZyWALL.
   2. Router>**enable**
   3. Router#**configure terminal**
   4. Router(config)#**setenv-startup stop-on-error off**
   5. Router(config)#**write**
   6. Load the older firmware to ZyWALL using standard firmware upload procedure.
   7. After system upload and boot-up successfully, login into ZyWALL via Console/Telnet/SSH.
   8. Router>**enable**
   9. Router#**write**

Now the system is successfully downgraded to older version.

Note: ZyWALL might lose some configuration settings during this downgrade procedure. It is caused by configuration conflict between older and newer firmware version. If this situation happens, user needs to configure these settings again.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

Appendix 2. SNMPv2 private MIBS support

SNMPv2 private MIBs provides user to monitor ZyWALL platform status. If user wants to use this feature, you must prepare the following step:

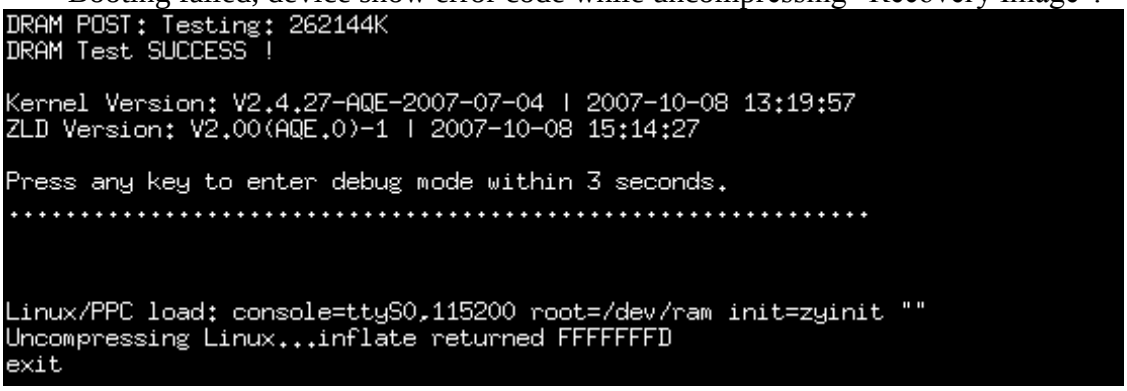
1. Have ZyWALL mib files (zywall.mib and zyxel-zywall-ZLD-Common.mib) and install to your MIBs application (like MIB-browser). You can see zywallZLDCommon (OLD is 1.3.6.1.4.1.890.1.6.22).
2. ZyWALL SNMP is enabled.
3. Using your MIBs application connects to ZyWALL.
4. SNMPv2 private MIBs support three kinds of status in ZyWALL:
   (A) CPU usage: Device CPU loading (%)
   (B) Memery usage: Device RAM usage (%)
   (C) VPNIpsecTotalThroughput: The VPN total throughput (Bytes/s), Total means all packets(Tx + Rx) through VPN.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

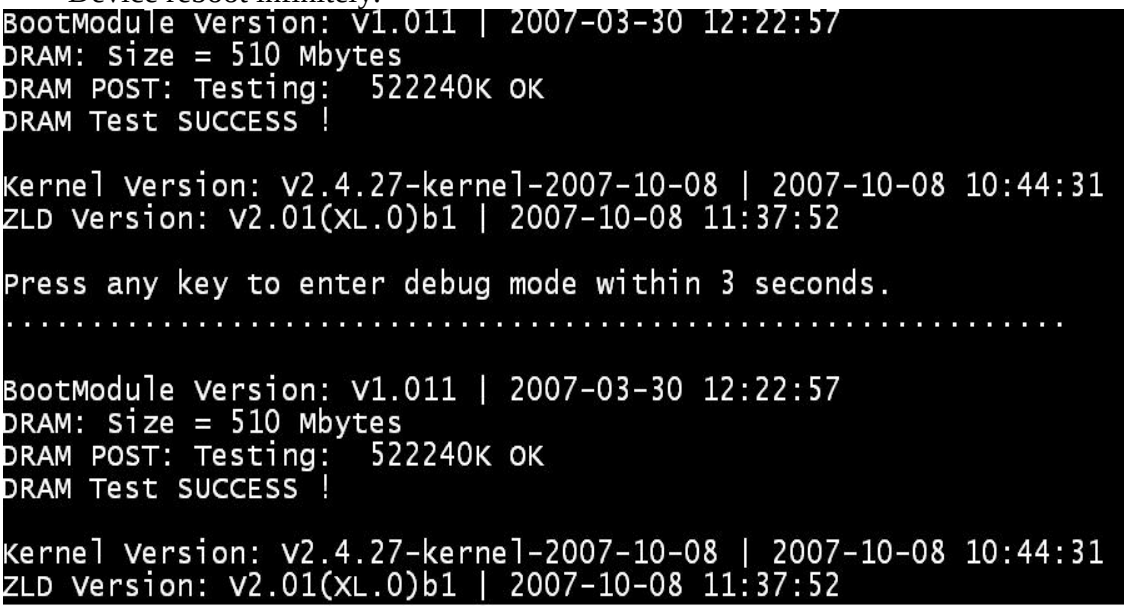
Appendix 3. Firmware Recovery

In some rare situation, ZyWALL might not boot up successfully after firmware upgrade. The following procedures are the steps to recover firmware to normal condition. Please connect console cable to ZyWALL.

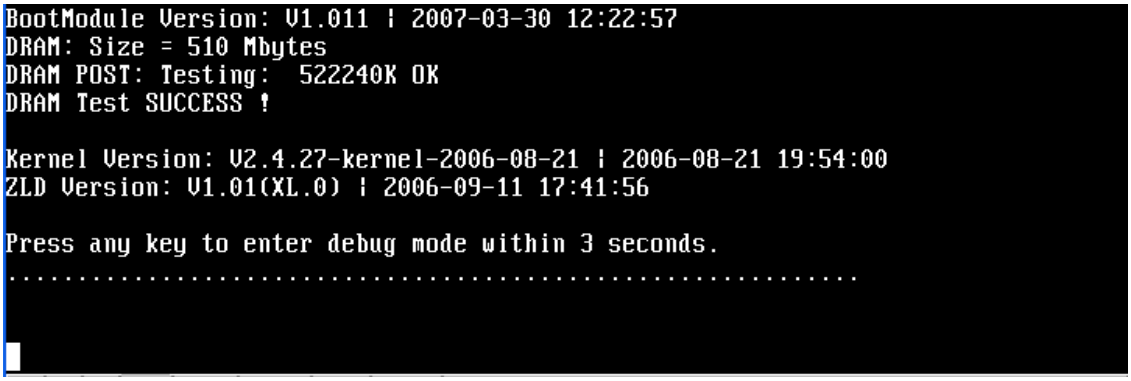
1. Restore the Recovery Image
   - If one of the following cases occur, you need to restore the "recovery image"
     - Booting failed, device show error code while uncompressing "Recovery Image".


DRAM POST: Testing: 262144K
DRAM Test SUCCESS !
Kernel Version: V2.4.27-AQE-2007-07-04 | 2007-10-08 13:19:57
ZLD Version: V2.00(AQE.0)-1 | 2007-10-08 15:14:27
Press any key to enter debug mode within 3 seconds.
Linux/PPC load: console=ttyS0,115200 root=/dev/ram init=zyinit ""
Uncompressing Linux...inflate returned FFFFFFFD
exit

     - Device reboot infinitely.


BootModule Version: V1.011 | 2007-03-30 12:22:57
DRAM: Size = 510 Mbytes
DRAM POST: Testing: 522240K OK
DRAM Test SUCCESS !
Kernel Version: V2.4.27-kernel-2007-10-08 | 2007-10-08 10:44:31
ZLD Version: V2.01(XL.0)b1 | 2007-10-08 11:37:52
Press any key to enter debug mode within 3 seconds.
BootModule Version: V1.011 | 2007-03-30 12:22:57
DRAM: Size = 510 Mbytes
DRAM POST: Testing: 522240K OK
DRAM Test SUCCESS !
Kernel Version: V2.4.27-kernel-2007-10-08 | 2007-10-08 10:44:31
ZLD Version: V2.01(XL.0)b1 | 2007-10-08 11:37:52

     - Nothing displays after "Press any key to enter debug mode within 3 seconds." for more than1 minute.


BootModule Version: V1.011 | 2007-03-30 12:22:57
DRAM: Size = 510 Mbytes
DRAM POST: Testing: 522240K OK
DRAM Test SUCCESS !
Kernel Version: V2.4.27-kernel-2006-08-21 | 2006-08-21 19:54:00
ZLD Version: V1.01(XL.0) | 2006-09-11 17:41:56
Press any key to enter debug mode within 3 seconds.

     - Startup message displays "Invalid Recovery Image".

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

```
BootModule Version: V1.012 | 2007-05-10 21:05:27
DRAM: Size = 510 Mbytes
DRAM POST: Testing:  522240K OK
DRAM Test SUCCESS !

Kernel Version: V2.4.27-XL-2007-05-10 | 2007-05-10 02:15:31
ZLD Version: VZW1050_DailyBuild_New_Trunk | 2007-05-10 03:12:49

Press any key to enter debug mode within 3 seconds.
.....................................................


Invalid Recovery Image

ERROR

Enter Debug Mode

>
```

- The message here could be “Invalid Firmware”. However, it is equivalent to “Invalid Recovery Image”.

```
Invalid Firmware!!!

ERROR
```

- Press any key to enter debug mode

```
BootModule Version: V1.011 | 2007-03-30 12:22:57
DRAM: Size = 510 Mbytes
DRAM POST: Testing:  522240K OK
DRAM Test SUCCESS !

Kernel Version: V2.4.27-kernel-2006-08-21 | 2006-08-21 19:54:00
ZLD Version: V1.01(XL.0) | 2006-09-11 17:41:56

Press any key to enter debug mode within 3 seconds.
.............................
Enter Debug Mode

>
```

- Enter atuk. The console prompts warning messages and waiting for the confirmation. Answer ‘Y’ and start to upload “recovery image” via Xmodem.

```
> atuk
This command is for restoring the "recovery image" (xxx.ri).
Use This command only when
1) the console displays "Invalid Recovery Image" or
2) the console freezes at "Press any key to enter debug mode within 3 seconds"
   for more than one minute.

Note:
Please exit this command immediately if you do not need to restore the
"recovery image".

Do you want to start the recovery process (Y/N)? (default N)
```

- Use the Xmodem feature of terminal emulation software to upload the file.
- Wait for about 3.5 minutes until finishing Xmodem.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

```
Total  2120704 bytes received.
programming ..........................................................
..........................................................
..........................................................
..........................................................
..........................................................
..........................................................
..............................................

OK

> 
```

- Enter atkz –f –l 192.168.1.1 performing the “Restore Firmware” process.

```
>
>
>
>
> atkz -f -l 192.168.1.1
```

- Enter atgo to bring up the FTP server on port 6

```
> atgo
Booting...
```

2. Restore Firmware
   - If “Connect a computer to port 6 and FTP to 192.168.1.1 to upload the new file” displays on the screen, you need to recover the firmware by the following procedure.

```
Connect a computer to port 6 and FTP to 192.168.1.1 to upload the new file.
```

   - You will use FTP to upload the firmware package. Keep the console session open in order to see when the firmware recovery finishes.
   - Set your computer to use a static IP address from 192.168.1.2 ~ 192.168.1.254. No matter how you have configured the ZyWALL’s IP addresses, your computer must use a static IP address in this range to recover the firmware.
   - Connect your computer to the ZyWALL’s port 6 (the only port that you can use for recovering the firmware).
   - Use an FTP client on your computer to connect to the ZyWALL. This example uses the ftp command in the Windows command prompt. The ZyWALL’s FTP server IP address for firmware recovery is 192.168.1.1
   - Log in without user name (just press enter).
   - Set the transfer mode to binary. Use “bin” (or just “bi” in the Windows command prompt).
   - Transfer the firmware file from your computer to the ZyWALL (the command is “put 1.01(XL.0)C0.bin” in the Windows command prompt).

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220-=(<*>)=-.:. (( Welcome to PureFTPd 1.0.11 )) .:.-=(<*>)=-
220-You are user number 1 of 50 allowed
220-Local time is now 03:21 and the load is 0.00. Server port: 21.
220-Only anonymous FTP is allowed here
220 You will be disconnected after 15 minutes of inactivity.
User (192.168.1.1:(none)):
230 Anonymous user logged in
ftp> bin
200 TYPE is now 8-bit binary
ftp> put E:\ftproot\ZLD_FW\101XL\101XL0C0\1.01(XL.0)C0.bin
```

   - Wait for the file transfer to complete.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.

```
200 PORT command successful
150 Connecting to port 3675
226-213.7 Mbytes free disk space
226-File successfully transferred
226 1.057 seconds (measured here), 33.06 Mbytes per second
ftp: 36642350 bytes sent in 1.06Seconds 34503.15Kbytes/sec.
ftp>
```

- The console session displays “Firmware received” after the FTP file transfer is complete. Then you need to wait while the ZyWALL recovers the firmware (this may take up to 4 minutes).

```
Firmware received ...

[Update Filesystem]
        Updating Code
        ..
```

- The message here might be “ZLD-current received”. Actually, it is equivalent to “Firmware received”.

```
ZLD-current received ...

[Update Filesystem]
        Updating Code
        ..
```

- The console session displays “done” when the firmware recovery is complete. Then the ZyWALL automatically restarts.

```
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
.....
        done

[Update Kernel]
        Extracting Kernel Image
        ..
        done
        Writing Kernel Image ... done
Restarting system.
```

- The username prompt displays after the ZyWALL starts up successfully. The firmware recovery process is now complete and the ZyWALL is ready to use.

© Copyright 1995-2013, ZyXEL Communications Corp. All rights reserved.